UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	No. 2:11-cr-00070-RAJ
	)	
	)	
vs.	)	Seattle, WA
	)	
ROMAN V. SELEZNEV,	)	
	)	Jury Trial, Day 7
Defendant.	)	August 23, 2016

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE JUDGE RICHARD A. JONES
UNITED STATES DISTRICT COURT

APPEARANCES:

FOR THE PLAINTIFF:

NORMAN McINTOSH BARBOSA
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
norman.barbosa@usdoj.gov

C. SETH WILKINSON
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
seth.wilkinson@usdoj.gov

HAROLD W. CHUN
U.S. Department of Justice
1301 New York Avenue NW, Suite 600
Washington, DC 20005
harold.chun@usdoj.gov

FOR THE DEFENDANT:

JOHN HENRY BROWNE
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
johnhenry@jhblawyer.com

EMMA SCANLAN
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
emma@jhblawyer.com

Andrea Ramirez, CRR, RPR
Official Court Reporter
United States District Court
Western District of Washington
700 Stewart Street, Suite 17205
Seattle, WA 98101
andrea_ramirez@wawd.uscourts.gov

Reported by stenotype, transcribed by computer

INDEX

EXHIBITS

THE CLERK: We are resuming our jury trial in the matter of the United States vs. Roman Seleznev, Cause Number CR11-70 assigned to this court.

THE COURT: Counsel for the government, please call your next witness.

MR. WILKINSON: The United States calls Mr. Steve Bussing.

THE COURT: Please step forward, sir.

THE CLERK: Please raise your right hand.

STEVEN BUSSING, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: It's Steven Bussing, B-U-S-S-I-N-G.

THE COURT: You may inquire.

MR. WILKINSON: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. WILKINSON

Q Good morning, sir.

A Good morning.

Q Can you tell the jury what you do for a living?

A My wife and I own a pizza place in Duvall, Washington.

Q And what's the pizza place called?

A Red Pepper Pizzeria.

Q Where is Duvall, Washington?

A It's east of Bellevue and Redmond.

Q How long have you been running Red Pepper Pizza?

A About five-and-a-half years.

Q And how many employees does the restaurant have?

A We have about 28.

Q I'm going to ask you some questions about your business a couple years ago, in 2014.

Was the business accepting credit cards at that time?

A Yes, we were.

Q And did you have a point-of-sale system that allowed you to do that?

A Yes, we did.

Q About how many cards were you processing daily at that time?

A On a guess, it's probably 100, give or take.

Q And I take it you have software that allowed the point-of-sale system to run?

A Yes.

Q In the event that maintenance needed to be done, or it needed to be fixed, who was responsible for performing that maintenance?

A I would call a helpline that we contracted for, with the POS company, which was 24 hours, to do any maintenance issues.

Q Okay. And would they access the computer by coming to your restaurant, or would they do it remotely?

A They would do it remotely.

Q At some point in time, did you see -- or witness anything that led you to believe that your point-of-sale system had been compromised?

A Yeah. One morning, I came in and noticed that the cursor was moving around on the screen of the back-office computer. And when I noticed that, somebody was trying to open up a web browser and download something. And then I literally pulled the plug, at that point.

Q Is that something you'd ever seen before?

A Correct.

Q It was not something you'd ever seen before?

A That's correct. I hadn't seen that before.

Q Okay. Did anyone have your permission to be in there, moving the cursor around?

A No, they did not.

Q So you said you pulled the plug of the machine.
What did you do next?

A I then called the POS support line to determine if they had been accessing it, for some reason. And they assured me that they had not, and they wouldn't without our express permission.

Q At some point in time, did you learn that credit card numbers had actually been obtained from your computer that way?

A Yeah. Right along in that same time frame, the credit card processor, Heartland, had contacted us and said that --

MR. BROWNE: Objection, Your Honor.

THE COURT: Sustained.

BY MR. WILKINSON

Q After you spoke with the credit card processor, did you understand that the system had actually been compromised?

A Yes. They told us that there were a number of cards that had --

MR. BROWNE: Objection.

THE COURT: Sustained.

BY MR. WILKINSON

Q So you said you pulled the plug.

Did you do anything to switch your system immediately, after you saw the cursor moving around?

A Yeah. It was in that day or two that we went to the credit card terminal as the exclusive point where we would enter credit card information, which was a dial-up connection, over the phone line.

Q And how did that work for you, for your business, compared to having the point-of-sale system?

A Well, we had to -- instead of using three terminals to process credit cards, we had that one single point, which caused a lot of congestion with dealing with customers, having to put them on hold and so forth.

Q What did you do with the point-of-sale system once you took it down?

A Well, we immediately got into the process with the POS provider to get a new system, so that we would have everything that was current. That system was about three years old, but we wanted to make sure that we weren't going to be compromised any longer and there was no vulnerabilities.

Q Were you planning to upgrade your system before this happened?

A Not specifically, no.

Q So as a result of this, sounds like you did upgrade your system?

A Yes. We put a rush on it and got it installed in the -- within a two-week period, I believe it was.

Q And how much did it cost you to upgrade the system?

A The actual cost of the system itself was in the neighborhood of $12,000.

Q At some point, were you contacted by law enforcement about viewing your point-of-sale system?

A Yeah. After we had -- did the upgrade, I had the old system stored at my house. And the Secret Service had come and asked if they could analyze those computers.

Q And did you agree to let them analyze it?

A Yes.

Q And do you remember the name of the agent?

A Agent Fischlin, I believe.

MR. WILKINSON: No further questions for this witness.

THE COURT: Cross examination?

MR. BROWNE: No questions.

THE COURT: Any objection to this witness being excused, by the government?

MR. WILKINSON: No, Your Honor.

THE COURT: By the defense?

MR. BROWNE: No, Your Honor.

THE COURT: Thank you, sir. You're excused. You may step down.

Counsel, next witness?

MR. BARBOSA: The government calls Chris Doyle.

THE COURT: Please step forward, sir, all the way to the front of the courtroom.

THE CLERK: Please raise your right hand.

CHRISTOPHER DOYLE, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Christopher Doyle, D-O-Y-L-E.

THE COURT: You may inquire.

////

DIRECT EXAMINATION

BY MR. BARBOSA

Q Good morning, Mr. Doyle.

A Good morning.

Q Where do you work?

A I own an Irish pub on the coast of Washington.

Q How long have you been on the coast of Washington?

A About five years.

Q Where were you living before that?

A Seattle.

Q Did you have different employment then?

A I did. I was a chief operating officer for a restaurant pizza company.

Q What restaurant pizza company?

A MAD Pizza.

Q And you said there were four of those?

A Four locations.

Q Where were those located?

A Madison Park, First Hill, South Lake Union, and Starfire.

Q And --

A In Renton.

Q Where is the Starfire location?

A It's located in the soccer complex, down in Renton, Washington.

Q And the First Hill location and the others, are those in

Seattle?

A They are.

Q MAD Pizza, did your business accept credit cards?

A We did.

Q How did you accept credit cards? What type of system?

A We had a swiper through our POS.

Q Were you familiar with the type of POS system you had at MAD Pizza?

A Firefly, by Phoenix. Or Phoenix, by Firefly.

Q How did that work at each of your locations? What did it consist of, in terms of the system and the architecture; do you recall?

A Well, we had two systems per location. Madison Park had three, actually, because delivery was pretty big down there. And, you know, it's your standard touchscreen, connected to a modem.

Q Did you have computer servers in the business?

A We did.

Q And terminals at the registers?

A Correct.

Q How was that system serviced if you had problems with it?

A Well, typically, it was done through the -- you know, on the phone and through the internet, by the help desk.

Q When you say through the internet, how would your --

A Well, they would dial into the system remotely.

Q Okay. Do you know approximately how many credit card transactions you were processing at each of your locations on a day-to-day basis?

A Gosh, probably running about 70 percent. I mean, it would just be a total guess, but I would probably say, you know, a hundred or more.

Q I'd like to draw your attention to late 2010, early 2011.

Did you learn that your business had been the victim of a point-of-sale intrusion?

A I did.

Q How did you learn about that?

A My operations manager called me at the office and said the Secret Service and the FBI were at the door, and they wanted in. We hadn't quite opened yet.

Q Okay. What did you do in response to that?

A I came down to South Lake Union to speak with them.

Q And what happened after that? What did you learn?

A They told me that --

MR. BROWNE: Objection, Your Honor.

THE WITNESS: They told me --

MR. BROWNE: Objection.

THE COURT: Sustained.

BY MR. BARBOSA

Q How many locations were impacted?

A Four.

Q What did you have to do in response to these intrusions?

A Well, we had to allow them to copy our hard drives, and then we had to send them off to a forensic scientist lab, one of 11 that they gave us a choice of, to have those analyzed, and then have them wiped clean and then sent back to us.

Q Did you send your drives, your systems, for all four of your locations?

A We did.

Q And do you recall who or what company you hired to do that?

A I don't.

Q Do you recall the cost of that?

A It was about $21,000.

Q For the four locations, total?

A Four locations.

Q Were there any other costs associated with the intrusions?

A We got fined from Visa and MasterCard, $10,000 from Visa, about 7,000 -- or $4,000 from MasterCard.

Q Were there any other impacts on your business?

A Well, we got some negative press, certainly. KIRO News showed up at one of the restaurants and --

MR. BROWNE: Objection.

THE WITNESS: -- you know, we were interviewed --

THE COURT: Just one second.

Grounds, Counsel?

MR. BROWNE: Relevancy.

THE COURT: It's overruled.

THE WITNESS: So, I mean, that wasn't flattering. What kind of impact it had, I'm not sure. It was really more of a situation where, you know, those funds were going to be used for upgrading restaurants, helping employees. We couldn't do that.

MR. BARBOSA: No further questions, Your Honor.

THE COURT: Cross examination?

MR. BROWNE: Yes, Your Honor.

CROSS EXAMINATION

BY MR. BROWNE

Q Good morning, sir.

A Good morning.

Q So you were -- just to make this clear, you were fined -- or the business you were working for then, you don't work for them anymore?

A I don't.

Q Okay. Were fined for not being PCI compliant?

A Well, apparently, that is the case, but that -- we understood that we were PCI compliant.

Q I understand.

A Right.

Q But once it was determined you were not, that's where the fines come in from MasterCard and Visa; right?

A Well, I don't know if those were the exact words that were used to me, but -- because I went through our processing company, Gravity, that helped me through that whole process. We didn't have an attorney. So I guess that is probably correct.

Q So the hacking, or whatever happened, brought this matter to your attention somehow. And then there was a fine, because you weren't PCI compliant. It wasn't the hacking that caused the fine. It was the fact that you were not PCI compliant.

Or is that a really complicated question?

A Well, it's not that complicated. But, you know, regardless if we were PCI compliant or not, we were hacked.

Q Okay. I understand that. So I think that's a "yes" to my question.

The new system was PCI compliant?

A The new system. We kept the same system. We had backup hard drives that we were able to use. And once we got hacked, we contacted the company, and they had an upgraded VPN router that we had to purchase to the tune of about 1,200 bucks per restaurant.

Q Okay. How many restaurants, again?

A Four.

Q Thank you, sir. That's all I have.

A You're welcome.

THE COURT: Redirect?

MR. BARBOSA: No, Your Honor. Thank you.

THE COURT: Any objection to this witness being excused, by the government?

MR. BARBOSA: No, Your Honor.

THE COURT: By the defense?

MR. BROWNE: No, Your Honor.

THE COURT: Thank you, sir. You may be excused.

Counsel for the government, your next witness?

MR. WILKINSON: The United States calls Sid Fanarof.

THE COURT: Please step forward, sir, all the way to the front of the courtroom.

THE CLERK: Please raise your right hand.

SIDNEY FANAROF, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Sidney Fanarof, F-A-N-A-R-O-F.

THE COURT: You may inquire.

MR. WILKINSON: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. WILKINSON

Q Good morning, sir.

A Good morning.

Q What do you do for a living?

A I'm president of ZPizza Corporation and founder of ZPizza International Corporation.

Q How long have you been running ZPizza?

A Thirty years.

Q How many pizza restaurants are associated with ZPizza?

A At one time, we had 90 franchise stores. And I own -- and ZPizza owned five stores, as well, personally.

Q Do you own five today?

A Yes.

Q In 2010, did you also own five?

A I owned, actually, six.

Q And where are the stores that you own located?

A Orange County.

Q Orange County, California?

A Yes.

Q How many employees did your stores have?

A About 70 to 80 at the time.

Q And were you accepting credit cards at that time?

A Yes, I was.

Q Through a point-of-sale system?

A Yes, I was.

Q And how was maintenance performed on that system? Was it done by people coming off site, or services accessing it from off site [sic]?

A Services off site. It was all done through the POS company, where they would update and handle that type of service.

Q Okay. So would they remotely access the computers?

A Yes, correct.

Q Do you remember the name of the POS company that would provide that service?

A It changed, but I think it was Firefly or Revention, or something like that.

Q Turning your attention to early 2011, did you learn that the point-of-sale system had been compromised?

A Yes, I did.

Q And how did you learn that, and without going into the specifics of what anyone told you as what was the source of the information?

A It came through my corporate office. We got a memorandum there from, I believe, the Firefly company, itself, stating it and --

MR. BROWNE: Objection, Your Honor.

THE COURT: Sustained.

Next question?

BY MR. WILKINSON

Q Were there costs to your business as a result of this compromise?

A Yes.

Q And did one of those involve having to perform an audit?

A Yes, it did.

Q And was the audit something you did voluntarily, or was it something you were required to do?

A Required.

Q Who paid for the audit?

A Personally, yeah.

Q And how much did it cost?

A It was, I believe, $5,500 per store, so it was about $30,000 for the audit.

Q Were any fines imposed on your stores?

A Yes. Approximately, I think, somewhere around 30-something from Visa and MasterCard. It was a settlement.

Q Did you also incur legal fees responding to this?

A Yes.

Q And how much were the legal fees?

A Maybe somewhere around $5,000.

Q At some point, did it become public that your stores had been intruded into?

A Yes.

Q And did that have any effect on your business?

A Yes.

Q And how would you generally describe that?

A Well, it was customers calling, who were concerned; and following that, people reluctant to use credit cards in our stores. And I don't know what the bottom line of that was.

But for a while, it was fairly strenuous with customers -- there was an article in the local paper that came out.

Q Generally, how would you describe sort of the overall cumulative effect of all of this on your business?

A Well, the effect on the business was horrendous. Because not only did I incur thousands upon thousands of dollars in costs, it happened at a time where there was another litigation going on, which I prevailed in, that was sort of frivolous, but so it -- the overwhelming thing was, I had a nervous breakdown. And to this day, I can't stand -- four years I was gone --

MR. BROWNE: I'm sorry, sir, to interrupt you.

I'm going to object on relevancy grounds. We talked about this.

THE COURT: I think we did cover this, Counsel.

MR. WILKINSON: Yes, Your Honor --

THE COURT: Objection is sustained.

MR. WILKINSON: Okay. No further questions, Your Honor.

THE COURT: Cross examination?

MR. BROWNE: Nothing, Your Honor.

THE COURT: Any objection to this witness being excused, by the government?

MR. WILKINSON: No, Your Honor.

THE COURT: By the defense? Counsel?

MR. BROWNE: I'm sorry. I was talking to

Ms. Scanlan. I apologize, Your Honor.

No, there is no objection.

THE COURT: Thank you, sir. You may step down. You're excused.

Counsel for the government?

MR. BARBOSA: Your Honor, the government rests.

THE COURT: Counsel for the defense?

MS. SCANLAN: Your Honor, if we may take a brief recess before we call our first witness?

THE COURT: Okay. Members of the jury, we'll take our first recess this morning while we engage in the transition between counsel for the government presenting their case and counsel for the defense.

Please rise.

(Jury exits the courtroom)

THE COURT: Counsel, just from a scheduling standpoint, approximately how much time do you think that your witness will --

MS. SCANLAN: About an hour.

THE COURT: About an hour? And any idea, Counsel, on cross examination?

MR. CHUN: Probably about the same, Your Honor.

THE COURT: Okay. So it looks like we'll be able to finish -- now, do you expect rebuttal testimony?

MR. CHUN: Likely, Your Honor.

THE COURT: And approximately how much time for rebuttal testimony?

MR. CHUN: Just on the the direct portions, Your Honor, an hour to an hour and a half.

THE COURT: Okay. So it looks like we'll occupy a full day today, with determining jury instructions this afternoon, as we previously discussed last week. And we'll do closing remarks first thing tomorrow morning.

Does that appear to be a fair goal for today?

MR. BARBOSA: Absolutely.

THE COURT: Counsel for the defense?

MR. BROWNE: Yes, Your Honor.

MS. SCANLAN: Yes, Your Honor.

THE COURT: We'll be in recess.

MR. WILKINSON: Your Honor, one quick thing, the last witness, I hadn't intended to elicit this testimony, but he did volunteer the statement about having an emotional breakdown. I don't know whether the defense would like an instruction to disregard it. We wouldn't object to it, at this point.

MR. BROWNE: No. As a matter of fact, to Mr. Wilkinson's credit, we talked about that before he took the stand. And counsel was not going to ask him that question, but I had a feeling the witness was going to get it out, one way or another, anyway. I don't want to highlight it at all.

THE COURT: If you want, I can -- I usually ask, Counsel, if you want the Court to strike testimony, tell the jury to disregard it, but I look for counsel to do two things: One, to object, and move to strike. So if I only hear the first part, which is "objection," without "move to strike," then there's no damage at that point. But if you don't want the instruction, you don't want the curative instruction from the Court, I won't give it.

Ms. Scanlan is shaking her head "no." I'm assuming Mr. Browne is agreeing with her.

MR. BROWNE: I usually do.

THE COURT: All right. We'll be in recess.

(Recess)

(Jury enters the courtroom)

THE COURT: Counsel?

MS. SCANLAN: Your Honor, the defense calls Eric Blank.

THE COURT: Please have him step forward.

THE CLERK: Please raise your right hand.

ERIC BLANK, having been duly sworn, was examined and testified as follows:

THE CLERK: Have a seat.

If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: It's Eric Blank, Eric with a "C," B-L-A-N-K.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MS. SCANLAN

Q Good morning, Mr. Blank.

A Hi.

Q What is your current occupation?

A I'm an attorney with a firm called Blank Law + Technology.

Q Is that a firm that you own?

A It is.

Q What does Blank Law + Technology do?

A We do computer forensics and document management investigations for governments and companies across the United States.

Q How long have you been doing that with this business?

A Since April 15, 2001.

Q And what are the types of clients you have? You said something about government agencies. Can you describe that?

A Well, so our clients are primarily large corporations. And by governments, I mean cities and counties, some state governments. I've done some work on the federal side for the Department of Defense. And in terms of the corporations, you know, Boeing, Microsoft, Yahoo!, AOL, companies like that, that hire us to come in and do investigations when they have some kind of computer-related crisis.

Q And what would be an example of a typical investigation that your company is asked to do for a corporate client?

A Well, say -- so recently, for example, for a city down in California, there was an allegation that a review of an employee had been fabricated and placed on the supervisor's computer. And so the investigation was, could we tell whether or not that document was, in fact, fabricated, and sort of been slipped onto the supervisor's computer or not.

Q Have you ever worked as a special master?

A Yes, I have.

Q And what is a "special master" in the context of your work?

A It's when the parties -- usually, the parties, but in other words, the parties to the lawsuit, or sometimes the Court without the parties really wanting the Court to do that, instruct me to undertake some investigation on behalf of the Court. So where I take on the position as a neutral, I'll do an investigation and then report back to the judge.

Q Have you ever been appointed as a special master within this district or this courthouse?

A Yes.

Q How many employees do you currently have?

A Twenty-three, including myself.

Q You said that you're an attorney.

What is your training in computer forensics?

A Well, I was -- I grew up as the computer person. I was the -- my junior high school's first computer lab aid. And I took a lot of computer classes in high school. I was part of a Massachusetts Institute of Technology special program they had to get people into the computer business. I built computers, back in the days where you used to build computers, instead of buy them at stores. I built computers for clients while I was in college. I did the same thing after college, when I was a police officer in Washington, D.C. And that's my background in computers.

Q Do you have any certifications in the computer forensic area?

A I have taken or taught all of the courses related to the major computer forensics tools. So AccessData's, what they call Computer Forensics Toolkit, which is what was used in this case. I've worked with that since 2001. I think I took their forensics boot camp in 2003. And I've taken a number of other computer forensics courses like that, where the manufacturers will put on seminars. I've been certified by Microsoft.

I had a business, until the end of 2014, that was a cybersecurity e-mail security business. It was the North American distributor for Google. And as part of being involved with that company, we -- I and others in my company had to go down to Google, and also to Intel, which they bought McAfee, which was another company, and get trained on the emerging issues of cybersecurity and threats across e-mail, and spoofing, and web filtering and protection, and so forth. So I've had quite a bit of continuing training.

Q What was that company called?

A One is Google, which is a big company, called Alphabet Now.

Q Sorry. What was the company called that you had, that did that work?

A Oh, I'm sorry. It was called TestudoData, like the Roman shield wall.

Q And TestudoData, you were talking about the training that you did in relation to that position.

What did your company do for Google and for those businesses that you just mentioned?

A Google had a distribution model where they employed -- or contracted, actually, with TestudoData to work with Google's resellers in North America who were reselling Google Message Security, Google Message Continuity, and other products that eventually became folded in to what we now call Google Apps for Business. In other words, if you were a person, you wouldn't buy directly from Google. You would buy from a reseller. The reseller would buy from TestudoData.

Q So before 2001, when you started Blank Law + Technology, what was your profession?

A I was an associate and then a partner at a law firm here in Seattle called Riddell Williams.

Q And did you handle cases involving electronic data litigation as an attorney?

A Yes. Now you see software is in everything. But at that time, the cases were Party A has paid Party B to build software to run a product that will build a prosthetic foot, and they have a dispute over how much of the product has been built, how much of the software has been built. And so you have to undertake an effort to get all that software back and determine what's been built or not built; so very complicated software cases.

Q And prior to being an attorney for that firm, and law school, what was your profession?

A Police officer, Washington, D.C.

Q I'm going to ask you now about the proper handling of electronic evidence.

What steps should be taken to secure a laptop computer that's seized, before you image it?

A Well, the first and most important rule always, really in seizing any evidence, but in computer evidence in particular, is to freeze it as you get it. Don't let any changes occur, to the extent you possibly can. There are always a few exceptions. But to the extent you possibly can, don't let that laptop or phone or tablet or desktop or server or whatever, don't let it keep making changes. Stop the changes so that you can ascribe or impute the contents of that computer to the person from whom you took it, and also so that it doesn't overwrite files that are beyond our forensic ability to recover them. Because although computer forensics is pretty amazing, in terms of what you can recapture, it's not perfect. It's an imperfect science.

Q So you want to freeze the item in the state that it's in at the time that you seize it?

A Right.

Q Okay.

A Normally, the process for that is to make an image, or bit-for-bit electronic copy, of whatever that device has that stores files. Usually, we say hard drives, with a computer, but it could be a solid-state drive, or a flash drive on a phone, and so forth. So once you have made an image of it, a forensically correct image, using tools, then you're okay, because then you know you've got that snapshot. So it's the interval between getting the thing and making --

MR. CHUN: Your Honor, objection. Narrative.

THE COURT: It is a narrative, Counsel. Let's ask another question.

BY MS. SCANLAN

Q So why is this -- why is this so important, that we not have any of these changes? Why do we care about that?

A Well, we care both offensively and defensively; in other words, offensively, because we want to make sure that we get everything that that computer had on it at the time we got it, and not have it lose anything. And on the defensive side, we want to be able to have that information be reliable; so just as you wouldn't take a notepad, and seize the notepad, and then leave it in a room, come back three hours later, you wouldn't know, had things been added to the notepad? How would you know?

It's exactly the same with a computer. So you freeze it so that you can be absolutely sure that the data on there is reliable and can be ascribed to the person from whom you took it. And that's not just me. That's the basic starting-off rule of computer forensics.

Q You said so that you don't lose anything from the device.

How do you lose things from a computer or tablet or an electronic item that you've seized?

A Well, computers, especially these days, are continuously operating and continuously connecting to the world. And when they do so, they write to files, and they will overwrite previously deleted items, or they'll make changes to files that might be significant in terms of what those files tell us about the computer's -- where the computer's been and what it's doing. So these changes occur even if no human does anything. These changes will keep on occurring, if you don't stop them from happening.

Q What does it mean that a file overwrites another file?

A Well, once a file is deleted, because computers -- if you think back to the dawn of computers, it's a lot of work for a computer to actually have to erase, scrub over, a deleted file. There would be no reason for it to do that. Instead, it simply flags that file as deleted, meaning that when you look for it, the flag alerts the program that you're using to look for it that, "Oh, that's a deleted file. Ignore it." But the file is still there and can be seen easily with forensic software.

The downside is that, as time goes on, since that file is deleted --

MR. CHUN: Objection. Same objection, Your Honor.

THE COURT: Same ruling, Counsel. Let's ask another question.

BY MS. SCANLAN

Q So you were just talking about how -- why we -- what overwriting is.

So when a file is deleted, then what happens -- how is it -- what is the overwrite process?

A Once a file has been marked for deletion, the normal operation of a computer will, sooner or later -- and this depends on how the computer operates -- overwrite that file, meaning to actually put new zeros and ones on top of the zeros and ones that were there in the deleted file. Then the deleted file becomes fragmented and is harder to recover. And eventually, it's gone altogether.

Q So what is -- what's encryption?

A Encryption is a method of making files unreadable to a person who doesn't have an encryption key.

Q Can you encrypt an entire computer?

A Yes. That's called "whole disk encryption."

Q So if you seize, or you take into your custody, a laptop that you're concerned that's encrypted, that's on when you seize it, what are -- what do you do with that computer from the time that you seize it, if you're worried that it's encrypted?

A So if it was encrypted, the only thing that you're going to get -- if you can't get past the encryption, and oftentimes you can't -- the only thing that you're going to be able to get is what's in RAM, the live memory that's on the actual surface of the motherboard, as opposed to on the hard drive. That RAM, if you can capture it, might actually have the encryption password.

Q So what do you do to -- what do you do with that?

A So if you do a -- it's called a "live RAM capture." You use software to try to grab the RAM, and then you analyze the RAM, and you look to see if there are words that look like passwords. And you try those out and see if -- usually, you try them out on an image -- and try them out and see if they work and get through the encryption.

Q Can you turn the battery off, or turn the computer off, before you try and do that, if something is encrypted?

A The whole difference between RAM and the actual storage is that RAM requires an electric current to be passing through it, in order to retain memory. So once the electric current stops flowing, the RAM dissipates forever. And turning the power off turns -- that means there's no electric current.

Q So do you need to leave it on, then, or can you turn it off?

A If you're going to do a live RAM capture, you should leave it on, not turn it off.

Q So is there an importance to when you try to do this live RAM capture? So does it matter if you try to do it immediately after you seize it or a month after you seize it?

A Yes, it does matter.

Q Why does that time frame matter?

A RAM is volatile, meaning it's constantly changing and moving. And that's where the computer is doing all its thinking. Grabbing it as soon as possible gives you your best chance at getting the password or any other data that's in RAM.

Also, back at the beginning of this, I said how important it is to take a snapshot of the computer as it exists right now. The longer you wait, the longer you're violating that first basic rule, which is, don't let the computer be changed. So grab it right away for those two reasons.

Q So if you leave it on, and you don't grab it right away, is the computer still making changes while it's on?

A Yes.

Q When -- what's the purpose of a Faraday enclosure?

A Faraday enclosures are designed to block radio transmissions.

Q So in the context of a computer where you're concerned that it might be encrypted, so you're going to leave it on, would you use a Faraday enclosure in that circumstance?

A Well, if the computer has any kind of wireless capability, you put it inside a Faraday enclosure until you've neutralized its wireless capability. That's just very common practice. And Faraday enclosures -- I mean, it sounds fancy and technical, but it's just grounded metal. We have, in my office, used metal trash cans that are just put on a cement floor. That works perfectly well. You don't have to buy some fancy thing.

Q So in theory, you could use anything like that, that's metal, and just put it over a laptop? Would that work?

A Yeah, and ground it.

Q And ground it. What does that mean?

A Connect it to the earth with something that conducts electricity, like metal.

Q So back in the summer of 2014, was your firm using Faraday enclosures for laptops?

A We had been, at that point, using Faraday enclosures for laptops and phones for years and years, yes.

Q So the idea of a Faraday enclosure for a laptop, was that breaking-edge, new stuff in 2014, or had it been around?

A I think "Faraday" is a term from World War II. It's a very old idea. Sort of the tinfoil hat thing is also the Faraday idea. So the idea of a Faraday enclosure is not new. And the idea that a phone uses a radio signal -- like a cell phone tower, that's a radio signal -- is also not new. So people have been using Faraday enclosures in computer forensics since as long as we've had cell phones; so that's since the '90s.

Q What about Faraday enclosures for laptop computers?

A Yeah, well, laptop computers, when they have wireless, that's a radio signal, different frequency than a cell tower. I guess I'm not -- I don't understand why you would treat it any differently. It's a walkie-talkie. Keep it from receiving signals, whether it's a desktop, which can have wireless cards in them, or a server or a laptop or a tablet or a phone. If it's got wireless capability, don't let it talk. That's just -- that's elementary.

Q Was that elementary in 2014, or just now?

A No. In 2000, it was elementary. The first wireless computers came out a decade and more before 2014. So, yes, you want to -- some computers had little mechanical on-off switches, with a little radio tower, for, like, the original, like, ThinkPads from 2007, for example. So you could just push that switch that turns off its wireless antenna. You could do that, instead of an enclosure. But if it doesn't have that, which most don't have it anymore, yeah, stop it from receiving radio signals.

Q So let's talk about Windows 8 and Windows 8 Pro.

First of all, what's the difference between Windows 8 and Windows 8 Pro?

A I think you mean Windows 8.1, which came out a year later than Windows 8.

Q Okay.

A Windows 8 is the next version of a Microsoft operating system. It followed Windows 7.

Q And when did Windows 8 come out; do you know?

A Yeah. Windows 8 was announced at the Consumer Electronics Show the first week of January 2011. I was at that show. It came out to early users later that year, and was released for general consumption, meaning that you really couldn't buy a computer anymore that didn't have it preloaded on it, in the early fall of 2012. And Windows 8.1 came out a year later.

Q And what's the difference between Windows 8.1 and -- or Windows 8 and Windows 8.1 Pro?

A There is not -- there's no operational difference between 8.1 and 8.1 Pro. They just have different settings and different capabilities. It's a more expensive version of

Windows 8.1, is all.

Q So at what point -- so it came out around fall 2012. At what point were the forensic tools available to analyze Windows 8 operating systems?

A So Windows 8 had been -- unlike other operating systems where people flee from them, and move to them at the last possible moment, Windows 8 was highly anticipated. And a lot of people, including my shop, moved to Windows 8 before its general release; unlike, say, Windows 10, where people had to be forced to sign up for Windows 10. So Windows 8 was popular and good.

The forensics tools do tend to lag behind a little bit, so I don't know exactly. But I think certainly FTK would have been on top of it. And I can remember working with Forensics Toolkit in 2012 on Windows 8 machines, so a couple months.

Q So in July of 2014, was it unusual to encounter a computer with a Windows 8 operating system within the field of computer forensics?

A No. Not in my experience, no.

Q So was that -- you said --

A Can I just add something to that?

The reason I want to say that is because the -- Windows 8 was the first version of Windows that was -- popularized this using the new touchscreen technology. So all the salespeople in the world, who tend to be involved in a lot of lawsuits, all wanted Windows 8, because that's how they would -- they're out in the field on their laptops that now have touchscreen capability. That's what Windows 8 brought. So most cases were immediately Windows 8 cases, because that -- if you had any kind of computer interest or skill, you wanted to leave your mouse and get on a touchscreen. If you were waiting tables, or a salesperson, or walking a factory floor, you wanted a touchscreen, and that was Windows 8, not Windows 7.

Q So if your company took custody of a computer with Windows 8 in the summer of 2014, would you have been familiar with the operating system at that point in time?

A Yes.

Q Were you -- is that unusual, within the field, just to your company, or is that a pretty general --

A I'm comfortable saying that's pretty general. I mean, we all -- I go to all these training things. I mean, Windows 8, as I said, was highly anticipated. So you moved into Windows 8 because that's what everyone was excited about showing up, because it meant, suddenly, like, you could use a Surface tablet with Windows 8 on it. So it was -- and so I'm not saying that hypothetically. I mean, I worked, in 2014, on a lot of Windows 8 machines.

Q And what is "Connected Standby" or "InstantGo"?

A Connected Standby came out with Windows 8, and InstantGo was how it was re-branded with Windows 8.1. Most of us, the people that I interact with, we still say "Connected Standby." It's just the preferred term. Connected Standby makes your computer act like a phone.

Q And what do you -- what do you mean it makes your computer act like a phone?

A Well, we're all familiar with a cell phone. The screen is dark, but you can still receive a call, or it will chime when e-mail arrives. That's because your phone is sleeping, using the minimal power, so it has 48 hours of sleep time. But it's not really sleeping. It's on the timer. And when the timer goes off, every 60 seconds or every 30 seconds, it wakes up long enough to say, "Hey, can I connect to a network?" "Am I connected to a network?" "Am I receiving e-mails or texts or incoming phone calls?" And you can even ping the connected standby machine and get it to wake up remotely. That's how your phone, which is dark, gets a phone call. And so with Connected Standby on Windows 8, you could do exactly the same thing with your computer.

Q Okay. So for the cell phone thing, specifically, you can -- if a phone is in Connected Standby -- and is the screen dark or on?

A Dark.

Q Okay. So it's dark. Can you send data to that phone in that state?

A Well, the answer is, yes, but it's first going to wake it up, although the screen may not turn on. So data, like an e-mail, an e-mail, when your phone's in that state, everyone's got a cell phone that goes "ping" when you just got an e-mail. The screen doesn't necessarily light up. You can set it to do that. But the screen may stay dark, but your phone will ping. You just had data pushed to your phone, even though it's in sleep mode, Connected Standby mode. And that's an example of data arriving on the phone.

Q And how about a laptop, is it the same or different?

A It's exactly the same. These days, phones tend to both connect to the radio network, which is the cell phone network, and they're also available to connect, of course, to the wireless networks, like at Starbucks. With computers, computers can connect to those wireless networks, but they have to have special extra hardware to connect to phone networks.

Q So if a computer wants to connect to a phone network, and it has a SIM card, will that SIM card allow it to do that, to have that radio capability?

A A SIM card with the hardware, yes. A SIM card is the subscriber identification module. It is what turns your computer into, actually, a phone, and you can send and receive phone calls, not Skype calls, but actually phone calls from the SIM card.

Q When did you first see laptops that had this Connected Standby capability?

A Windows 8. But that -- sorry. Built in came with Windows 8. But the idea of people using their laptops and having Connected Standby-type features, we started seeing those in 2007. But you had to buy -- it didn't come preloaded. You had to buy what we'd now call an "app" for that.

Q So Connected Standby was built in in Windows 8.

And when did Windows 8 come out, again?

A It was pre-release in 2011 and general release in October, I think, of 2012.

Q What precautions should be taken when you take custody of a laptop that has Windows 8 and Connected Standby capabilities?

A Treat it like a phone. Block the wireless signal. Make your image of it, your bit-for-bit electronic copy, as quickly as possible.

When I say "make the image," most of us will make two or more images, so then you've got perfect replica copies. And if something goes wrong, you've got backup. So make this backup, this forensic backup, as quickly as possible. And while you're doing that, stop it from connecting, either because there's some piece of hardware you can disconnect, or putting it in a radio-blocking cage, like a Faraday enclosure.

Q That process that you just talked about, is that new to 2016, or is that commonly known in the summer of 2014?

A It's commonly known in the summer of 2014 and earlier.

Q Now, switching over, we've heard a lot about event logs.

What is an event log on a computer?

A An event log is a document, like a Word file or a text file, where the computer writes down what it's doing or what has happened. And most computers have many different kinds of event logs.

Q And what's a "SRUM journal"?

A SRUM is just a power usage monitor. It's -- the big competition is to preserve battery power. So the System Resource Usage Monitor just tells you what's causing power to drain, so you can fiddle with it and try to make your computer last longer.

Q So event logs, are event logs on there for computer forensic people, like you, to look at, generally, or for diagnostic purposes?

A They're for diagnostic purposes. We use them in computer forensics all the time, but they're not built for that purpose.

Q Why are they there for diagnostics purposes? What does that mean?

A Well, take the SRUM journal. Everyone can understand that -- if you don't understand why your friend's laptop goes five hours before the battery dies, and your laptop goes three hours, one way to help diagnose that might be to pull up the SRUM and take a look at what's using power. And, oh, it turns out that you forgot you're connecting to this USB drive, that you should probably disconnect when you're not using it, because it's killing an hour of your laptop time. So that's user diagnostics.

Network diagnostics, many of these devices connected to each other will refer to each other's event logs to determine what they're supposed to do next, which is why, if you have problematic event logs, you can have cascading problems across the whole system, because everyone will rely on the faulty event log. And that happens commonly.

Q So these event logs, can they be changed or edited by a person?

A Yeah. In recent years, Microsoft has made an effort to have them not be changeable, not for computer forensics purposes, but because people tend to try to solve problems by just taking the danger signals -- so if I have a computer, and my printer is not working, my printer might be referring to an event log to do something wrong. So why don't I fix my printer by deleting a line item or changing a line item in my computer's event log, to help me diagnose the printer problem. That usually causes more harm than good. And so Microsoft has made an effort to stop people from being able to do that. But the people who want to do it will do it. And so it's not hard to change event logs.

Q How do you change -- how do you change an event log?

A Well, at the end of the day, they're just, like, how do you change a text file or a Word document? You open it up, you make the changes you want to make, and then you "save as," and you overwrite the prior one, and, voila, changed event log. It's just a document with lines.

Q So some of these -- do some of these event logs track whether a user is currently logged on or doing things on the computer?

A Some do. There are security event logs. There are wireless connection logs. Some apps create their own event logs to tell you what they're doing. So, yes.

Q So those event logs that -- you mentioned the security event log. There's the wireless connectivity log; right?

A Right.

Q Those ones that are recording user interaction, are -- can you edit those ones?

A Yes. There's no -- they're all in the same format. The computer uses the same processor, the same software, to write to various logs.

Q So if you look at those logs for a particular computer, and you don't see evidence the user is interacting, does that mean absolutely, a hundred percent, that that event didn't happen?

A No, it doesn't. And, I mean, we see this kind of -- computer forensics relies on surprise. You need to know that the person whose computer you're looking at doesn't know that you're coming, because they can make all these changes. And you'll never -- without -- so that's the human part of this. Without this careful preservation of the computer, and the chain of custody, you lose your human part of it, and you're just looking at an event log. How do you know it hasn't been changed? You don't. It's rare that it's changed, because usually you've surprised the person.

Q But you can't -- can you know for sure?

A No. And we see this just in our daily lives. I mean, I recently saw the head of the FBI say you can't be sure what's happened to this computer, because it's just not something you'd expect to be able to figure out, one way or the other. Well, why not? Why doesn't he just look at the event logs? Answer: That's not a trustworthy way to depend on a computer.

Q I think we may have talked about this, but can a laptop that has a SIM card connect to a radio network when it's in some kind of standby mode?

A Connected Standby, yes. That's its whole purpose. It will connect to whatever network -- the SIM card is a network-specific, like Verizon or AT&T Wireless, so you get a SIM card that's in that network. So that SIM card will give you permission to connect to anybody in that network.

Q Does it give you -- can it give you that permission even if -- give the computer the permission even if the user is not logged on?

A Yes, of course, just like a phone, works exactly the same as a phone. It will log on to trusted cell phone networks. And by default, if it's a Verizon Wireless SIM card, it trusts all Verizon cell towers, all "X" thousand of them across the country, and any carrier that Verizon trusts.

Q Did you examine a copy of the drive that was found in the Sony Vaio laptop in this case?

A Yes. I was given a forensic image by the government.

Q And that forensic image, do you know -- how was that created?

A The image is a bit-for-bit electronic copy. I don't recall -- I think they used FTK Imager, which is a perfectly fine forensic toolkit imager, which is a software program that allows you to make a copy. It's perfectly legitimate. We all use that. There are other things that work, as well. But you know it's a perfect copy because you compare -- you compare your copy to the original, using a hash procedure, and it tells you the same thing, and we trust it.

Q And once you received this image, what did you do to conduct your examination?

A I used Forensic Toolkit to index what we call -- which means build a total library of all the data on the computer, including deleted files and fragmentary files, and files that you wouldn't normally see using programs. And once I've done that, I can search and look at the various files. I can sort them. I can run word searches.

Q And did you find anything of note in your examination of this laptop?

A Yes.

Q What was that?

A That many thousands of files had had their metadata, that is, information about the files, changed after this computer was seized.

Q And what's your understanding of when this computer was seized?

A Sometime on July 5, 2014.

Q So you saw changes to the metadata that were after that?

A Yes.

Q What kinds of changes?

A There were changes to file access dates, and there were changes to file modification dates.

Q And what's an "access date"?

A An access date is a piece of information associated with a file that tells you when the file was last touched. What causes it to change varies from program to program. It might have been opened, printed. It could be changed, but doesn't have to be, and so forth.

Q Can that -- can access logs be changed by the computer itself, without a user?

A They can be, because apps themselves can change access dates, yes.

Q And can access dates also be changed by user interaction?

A Yes.

Q So these files that you saw with changed access dates -- can you take a look at Exhibit 114?

A Okay.

Q Take a look at that. Do you recognize that?

A Yes.

Q What is it?

A This is a condensed -- and by condensed, I don't mean it's missing files. I mean that it -- in Forensic Toolkit, you get a lot of information about each file, sometimes a hundred, 120. So if you look at this document, it could be 120 columns over, hard to print. So here, I've just shown the file name, the access date, and the modified date. But this is a document I created.

Q And what does it depict? So it has those columns. What is it telling us?

A I went into FTK and pulled up all files on the computer sorted by access date, from most recent to least recent. And then I cut off the ones that were prior to the computer being seized. So these are all the access dates of files that were changed after the computer was seized by the government.

Q And is that an accurate record of that information?

A Yes.

MS. SCANLAN: The defense moves to admit Exhibit 114.

THE COURT: Any objection?

MR. CHUN: No, Your Honor.

THE COURT: 114 is admitted.

(Exhibit 114 was admitted)

MS. SCANLAN: Permission to publish?

THE COURT: Granted.

BY MS. SCANLAN

Q This may be a little hard to see, but we're using the document camera today.

So what are we -- what is this? What is this? What is this column here, starting with "name"?

A Left column is the name of the file. Those are -- it's -- the next column is the access -- last access date. And this is a spreadsheet. It is sorted by access date. So you'll see the names are not in alphabetical order, but the access dates are in reverse chronological order, so most recent to least recent. And then the next, Column C, is the modification date from most recent to least recent.

Q Okay. Can you see that okay, in terms of those column names on the screen?

A I've got it. I'm looking at them --

Q Look at your screen.

A Okay. I'm looking at my screen.

Q Can you see these okay?

A Yes.

Q Sort of?

A Yes.

Q All right. Not all the technology is perfect here.
But here we have -- this is the "name" file; right?

A Yes.

Q And then these are the access dates, over here?

A Correct.

Q And so this column, are you saying that all of these dates in this column are after July 5?

A Yes.

Q How many pages is this?

A Sixty-one.

Q And how many files are we talking about?

A Somewhere in the neighborhood of 3,000 files, which is a lot.

Q Now, these changes in access dates on these files, is there any way to know whether these are caused by user activity, for sure, or system activity?

A In my opinion, having done a lot of work into this, these can only be caused by some kind of user activity, not by system activity.

Q Why is that?

A Well, because I'm very familiar with Connected Standby. And I guess I should say, I'm -- I get to this by looking at what the government said about this, which was nothing. And that made me wonder, how can I try to explain all of these files? Because it's kind of hard to miss them. There are thousands and thousands and thousands.

Q Wait. Hold on. Before you go on, what do you mean the government said nothing?

A Well, the government had a report about their forensic examination, and they said a few files, a few registry files, had been changed.

Q Are these registry files?

A No. Actually -- sorry. Some of them are; two, three, four of them are.

Q So there's two, three, four of these 3,000 files that are registry files?

A Right.

Q Are the rest of them a few registry files?

A No one would think that these are registry files.

Q Okay. And then I interrupted.

So you said it was your opinion that this is caused by user activity. Why is that?

A So one of my reasons was that I haven't had the computer. I've had an image of the hard drive on the computer. So I don't know firsthand, where's the computer been? Who's been touching it? Who's been opening it? Who's been accessing it? Who's it been talking to? I don't know anything but what I can see from the solid-state drive.

But I do know how Connected Standby works. And Connected Standby is meant to preserve battery life, allow your phone or computer to not drain battery. Thousands and thousands of files being accessed, whatever is happening to them, takes a lot of battery power. A computer in Connected Standby is not going to modify or access all of these files. So that -- I throw that out.

So if the computer is just sitting there, normally it will go into a Connected Standby state. So if it's doing all this work, and we know that, if it's left alone, it would go into Connected Standby, and we know that Connected Standby would not result in thousands and thousands of files being accessed, we conclude user activity. Or I conclude that this is some kind of user activity. What user activity, I can't tell.

Q Do you know how long the laptop was left in this condition before it was imaged?

A I think it's around 23 days.

Q Does that seem like a normal period of time to you to wait to image a computer that's in Connected Standby mode?

A If I took 23 days to image a computer, I would not have any clients. And in addition, it's not a normal time. It should be done emergency quickly. That's why we have all these portable imaging devices that we take with us to the scene, so we can do it, boom, right there.

Q Oh, so, like, the portable imaging devices, like the live image that Detective Dunn did on some of the business point-of-sale systems?

A Right. Because these businesses, they're in business. They can't let you take their computer away for three weeks, then come back and say, "Okay. Go ahead. You're back in business." Every minute -- you take someone's cell phone away, every ten minutes they want to know when they're going to get their cell phone back. So once you get the image done, they can get their cell phone back. Imagine taking 23 days before I return your cell phone.

Q Did you have a chance to look at the frequency of different dates for these 3,000 files?

A I did, and I made some graph as part of my analysis.

Q Can you look at Defense Exhibit 106, please? It's in the notebook.

A I see it.

Q Okay. What is it?

A This is -- as me trying to understand what's going on with this computer, I just took this same spreadsheet and, using Excel, turned it into a graph to show me, if you just take the days, does that tell me anything about the pattern of activity.

And I'd just like to say one thing. If you look at the very end, August --

Q Hold on. Nobody can see it yet. So right now, we're just identifying what it is.

So this is a graph you created?

A Right.

Q Is this an accurate representation of the file activity you saw on this computer?

A Yes. If you went through these 61 pages, you could reconstruct this graph by hand.

MS. SCANLAN: Defense moves to admit Exhibit 106.

MR. CHUN: No objection, Your Honor.

THE COURT: Is that for substantive or illustrative?

MS. SCANLAN: Substantive.

THE COURT: Objection is noted -- strike that. Government has no objection --

MR. CHUN: No objection, Your Honor.

THE COURT: 106 is admitted.

(Exhibit 106 was admitted)

MS. SCANLAN: Permission to publish?

THE COURT: Granted.

BY MS. SCANLAN

Q Okay. Another one of my ELMO features.

What are we looking at here?

A So this is the bar graph from Excel of the dates in 2014 post-seizure of the computer, so the 7/5/2014 dates, those are 7/5 dates after the computer was seized.

Q What's the last date?

A The last date is August 1. And that's what I wanted to point out, is that because -- if you look at the little tiny number there, it actually says "3." But you don't -- the bar, it's such a tiny number that you don't get any little blue graph.

Q So on the August 1 date?

A Yes, on the August 1 date.

Q Okay. So that has -- you can't really see it right here. It has three file changes; right?

A Because if you look at this prior exhibit, there are three dates from August 1.

Q And then this date with the big column in the middle, what's that date?

A July 13.

Q And how many files had access date changes on that day?

A 1,800-some.

Q Is it unusual that a computer that's in Connected Standby would have a spike like this, in the access date changes?

A If you mean would a computer in Connected Standby suddenly decide, after sitting there, to access nearly 2,000 files, that's not just unusual, that's just -- that's not how Connected Standby works.

Q Okay. So in terms of -- when we say "routine system activity," is that what we're talking about, where the computer is doing it itself, without a user?

A Right.

Q Okay. So would a computer that was showing this pattern of file activity, is this something you would generally ascribe to routine system activity?

A No. There's some kind of user interaction. A human being did something to cause this computer to do something else.

Q What about antivirus activity?

A In the old days, antivirus would -- you always suspect antivirus. Because in the old days, antivirus used to change last access dates. But it drove the industry crazy. And by 2009/2010, that wasn't happening anymore. This is McAfee. It's one of the first things I checked. This is McAfee Antivirus. I am overfamiliar with McAfee Antivirus. This is not McAfee Antivirus activity.

Q And let's back up a little bit.

What is McAfee Antivirus?

A It is an application that opens, without changing the modification date or the access date, files to inspect them to see if they have viruses, and then packages them back together, pastes back the original open access date, and goes on to the next file.

Q Okay. So -- and what is your experience with McAfee?

A In -- from 2005 to 2014, I sold about $50 million of it. So I've had -- every problem McAfee Antivirus could have, my shop has experienced, and had to endure.

Q Have you ever seen this kind of file activity caused by that antivirus program?

A Well, yeah, prior to 2009.

Q How about after 2009?

A No. Yeah, prior to 2009, McAfee would literally go through and change all your last access dates; so that when you went into Word, it would show your last access date was whatever the antivirus looked at, which was just crazy. But after 2009, as we all know from using computers today, if you go into Word, and you go to your recent files, it doesn't show you what was recently scanned by an antivirus. It shows you what you recently accessed. So after 2009, no, antivirus doesn't change last access dates.

THE COURT: Counsel, it's 10:45. Why don't we take our morning break at this time.

(Jury exits the courtroom)

THE COURT: Counsel for the defense, anything to take up?

MS. SCANLAN: No, Your Honor.

THE COURT: Counsel for the government?

MR. CHUN: No, Your Honor.

THE COURT: We'll be in recess.

(Recess)

(Jury enters the courtroom)

THE COURT: Counsel, you may continue your direct examination of the witness.

MS. SCANLAN: Thank you, Your Honor.

BY MS. SCANLAN

Q Mr. Blank, we were talking about this laptop.

Does this -- the laptop that we're talking about, that you looked at the image of, did it have a SIM card?

A Yes.

Q Is the SIM card something you get a copy of when you get the forensic image of the computer?

A No. It's a piece of hardware that attaches to the computer. It's a little chip.

Q Do you know when everybody figured out that this thing had a SIM card?

A I know when I figured it out.

Q When was that?

A Back in June of this year.

Q And where were you?

A Here, in this courtroom.

Q Prior to that time in June when we had the SIM card revelation, I'll call it, had you personally examined the actual computer?

A No. I only had access to the image the government had given me.

Q Do you know what company supports that SIM card?

A Yeah. It's MegaFon, which is not -- it's spelled a little bit different. It's F-O-N, for phone. It's the largest

Russian telecom company.

Q They're not in Seattle; right?

A Well, no, they're not.

Q Do you know if they have a partnership with Verizon?

A Yeah. They're part of the CCA, the Competitive Carrier Alliance, which allows companies to roam onto other networks. And their roaming partner in the U.S. is Verizon.

Q Verizon Wireless, like the Verizon that has a store, like, three or four blocks from here?

A Yeah. Verizon, like the one that has 50,000 towers in the U.S., yes.

Q So what does it mean that these are part of the -- what did you call it, the CCA network?

A It just means that if you fly in from Russia, and you have a Russia MegaFon SIM card, and you get off the plane, if you haven't told your phone not to, as has happened to some of us when we go to Mexico, for example, your phone will start roaming locally on Verizon. Your Russian phone, with the Russian SIM card, will work just fine here in the U.S. It will trust and connect to the Verizon network, as a roaming partner.

Q Now, you're talking about cell phones; right?

A I'm talking about anything that has a SIM card. The SIM card doesn't care whether it looks like a phone or laptop or desktop, or you're carrying around a big server. This same thing would apply to a cell phone; but, yes, also to a laptop or tablet, including this laptop.

Q So a laptop -- so are you saying that a laptop with a SIM card from MegaFon can connect to the Verizon trusted network in Seattle?

A Of course, yes.

Q And can it do that in Connected Standby, or only when a user is interacting with it?

A Connected Standby, the operative word is "connected." And it will try to connect to trusted networks. With a SIM card and MegaFon, it will trust MegaFon's network, and it will trust all of MegaFon's partner carriers. It will just trust them. So you can drive along the highway, and even though you're going from tower to tower to tower, you can have an uninterrupted cell phone conversation, uninterrupted e-mail, uninterrupted web surfing over MegaFon or their roaming partner, Verizon network.

So specifically what I'm saying is, this laptop, on, or in Connected Standby, brought to Seattle, would be expected to connect to the Verizon network here, just normally, without any user action at all.

Q So if it had been -- if the laptop with the SIM card was in some sort of Faraday enclosure or trash can, was grounded, or whatever you want to call it, would it be able to do that?

A No. It blocks the radio signal. It's like being in a tunnel.

Q But if it's not in any of those things, then that's when it's capable of making this connection?

A Yeah. Not just capable, but it will, unless told not to, try to make those connections. It will try.

Q Now, are you familiar with the wireless -- not just -- okay -- whatever the log is, the connectivity log, that records a SIM card or a radio network laptop's connection with a wireless network?

A Yes. It's one of those logs we talked about earlier.

Q And is this one of the logs that can be changed, or is it something that is inalterable?

A It's a text file, and it can be changed for all kinds of -- it can be changed easily.

Q So let's just be clear. Are you saying that that particular log on this computer was changed?

A No. I don't know.

Q So you don't know -- we don't know, one way or the other, whether it was changed or not?

A That's right. And that's what I'm -- what I'm saying is, I'm talking about reliability. I'm not saying what happened. I don't know. All I've got is an image of the hard drive of this computer. I don't know what the computer was or wasn't doing. I don't know.

Q So in terms of the reliability of this computer, or the evidence that's taken out of this computer, what is your opinion about that? I mean, how reliable is the stuff that's on this computer?

A My opinion is that the computer was handled in -- you don't get the thousands and thousands of access date changes without mishandling the computer. It's the basic principle of computer forensics that you secure the evidence, secure its -- just like any other evidence, secure the computer; prevent it from being changed, and prevent the possibility of change.

It did get changed. And we know, because the SIM card was discovered years later, that there's even more possibility of change than we see just from the hard drive itself. There's also this -- the fact that it's a walking-around phone.

So those two things, and all of my training and experience, lead me to my opinion, which is that this laptop, the data on it, is unreliable, from a computer forensic standpoint.

Q So what about -- the government's taken a group of files that don't have changed access dates and said, "These are the files we're using." What about those files? Those ones that don't have changed access dates, are they a separate set of evidence that is reliable?

A No. I mean, in computer forensics, when you're trying to see if someone's tampered with a computer or not, or maybe the computer tampered with itself -- I mean, that's always a possibility, that something's wrong -- you don't just look at the files you can find, that you can prove something changed. Once you find unexplained changes after the seizure date, if you can't explain those changes -- and some changes do happen. There are, even in this case, some changes that I think are well explained.

But when you have the thousands and thousands of changes, and nobody even mentions them, they're not even brought up, and then when they are brought up, there's no explanation, then everything is suspect. Because it just means that we don't know what happened to the rest of the files, just because we can't see the changes.

Q What are the well-explained file changes?

A I thought, initially -- when I read the report of the government on working with the laptop, initially, there was talk about bumping the computer, and it came back on accidentally. And I think -- look, I've been in computer forensics for a long time. You're not supposed to bump the laptop. You're not supposed to make it turn back on. But those things do happen. And if you can explain them, then it corrects the problem.

So I thought, and I think I said in my, you know, original report, that I find that persuasive. So, okay, that's three files out of 3,000. Why don't you even mention the rest of them?

Q So the three files out of 3,000, is that the thing we saw at the end of the graph, on August 1?

A Yes. Like I said, it's not ideal. I just want to be clear. Computer forensics is somewhat forgiving. You just need to explain your mistakes. When you explain your mistakes, okay. But to have mistakes and have them not be explained, everybody gets suspicious.

Q Have you heard the explanation that this is operating system activity or antivirus activity that's causing these file changes?

A I have.

Q So just to be clear, do you agree with that explanation, or not?

A No. It doesn't make any sense. It doesn't -- just from a practical point of view, no computer that's sleeping is going to be doing all this work. It's going to have to have been woke up at some point. And if it was doing all this work, why isn't it doing it every day? Why does it do a lot of work on one day and almost no work the other day? That doesn't make any sense that that's just how this computer operates. It's not supported by anything.

Q And how many hours would you say you've put into this case?

A Two-hundred-fifty.

Q Are you compensated for that time?

A Yes.

Q Is the compensation that you receive dependent on what your opinion is?

A No.

Q So if you say something we don't like, do you still get paid?

A That's a different question. Not always. I have been -- but, I mean, my concern is that what I say allows me to be hired in the next case. So I'm sorry to be so frank, but that's my -- I need -- I'm not going to put myself somewhere where it hurts my reputation as a computer expert. And it's not -- this case is not worth it to me, neither is any case.

Q What does that mean?

A It means that what I say is not --

MR. CHUN: Objection, Your Honor. Vouching.

THE COURT: It is, Counsel. Sustained.

MS. SCANLAN: I have nothing further.

THE COURT: Cross examination?

MR. CHUN: Thank you, Your Honor.

CROSS EXAMINATION

BY MR. CHUN

Q Good morning, Mr. Blank.

A Hi.

Q Are you still an attorney?

A Yes.

Q Are you still licensed?

A Yes.

Q Do you still practice law?

A I say yes.

Q And in this case, have you reviewed the reports?

A Which reports?

Q Agent reports.

A Yes. I've reviewed a number of reports, yes.

Q Forensic examination reports?

A Yes.

Q You've reviewed the forensic image of the defendant's laptop?

A Yes, I have.

Q Now, being both a forensic examiner and an attorney, that's one of your marketing points.

It's because you know how to be an advocate?

A I'm sorry?

Q It's a question.

A Oh, okay. I think that it's helpful to -- not so much the advocacy part, but I think it's important to know the law and be able to understand how the law connects to the facts. I think it's been useful over the years, yes.

Also, I deal with extremely sensitive information. And I think it makes clients more comfortable, knowing they have some of the protections that an attorney can provide them.

Q And you put this in your report, that you've personally both worked as an examiner and an advocate; correct?

A Yes.

Q And in your report, you use the word "advocate," not "attorney"; right?

A Okay. Yes.

Q And you write your report to that, because --

MS. SCANLAN: Objection. I'm going to object to questions about the report. He can ask a question and impeach with the report, but I'm not sure about the questions directly about what's in the report.

THE COURT: That's overruled. I'll make a determination based on a question-by-question basis, Counsel. But the general global objection, that's overruled.

Please continue.

BY MR. CHUN

Q And you write your reports as advocacy pieces; correct?

A I guess I don't really know how to answer that. I mean, I think it's fair to say that I'm hired by a side, and I try to help that side. But I don't say stuff that's not defensible. I guess -- is that enough of an answer?

Q For example, in your March 1 report, you say, "According to the investigating agency, Mr. Seleznev had a laptop"; isn't that right, paraphrasing?

A That's correct. That makes sense. I'm explaining where I got the information from.

Q You didn't believe he has a laptop?

A No. I believe he had a laptop.

Oh, I see. No, I'm not saying it in some sarcastic tone. I'm just explaining where I got the information from, in terms of how do I know that he had a laptop, because the investigating agency tells me.

Q So you've reviewed the discovery, and so you're familiar with this picture?

A This is the first time I've seen that picture.

Q He's carrying a laptop bag there?

A I don't disagree with you. I can't -- to be honest, I don't even -- yeah, I've never seen the picture before. I don't disagree with what you're saying, but I can't tell what he's carrying or -- in fact, I'm having a little trouble seeing who that is --

THE COURT: Counsel, to preserve the record, if you could point to the exhibits.

MR. CHUN: I apologize, Your Honor. That would be Exhibit 12.2, Page 2.

BY MR. CHUN

Q And showing you now what's been admitted as 12.4, is that a picture of the laptop there?

A Oh. I see a bunch of stuff, including what looks like a laptop, yes.

Q And showing you the bulk exhibit, Exhibit 12.8, which is the laptop, if it's up there.

MR. CHUN: Ms. Ericksen, 12.8?

THE CLERK: The laptop?

THE WITNESS: This is the first time I've touched this laptop.

BY MR. CHUN

Q Looks like what's in the picture?

A Yes.

Q And so you believe that's the defendant's laptop?

A I have no reason to doubt it.

Q Another example of advocacy, in your report, you say, in parentheses, in regards to Indonesia -- or in parenthetical -- "where Mr. Seleznev apparently traveled."

Were you not aware that he traveled to Indonesia? Or do you not believe it?

A So when I write my reports, and I think -- I also was trained to do this as a police officer -- I try to separate what I've heard from what I know from personal observation or facts. So I realize -- I mean, maybe policing is not the best place to learn to write reports, but that was always -- if you get information from a third-party source, that's not something I'm stating as fact. It doesn't mean I'm disbelieving anyone. But there are facts that I observe from my own eyes. You'll get those as facts. Everything else, I'm going to tell you where I got it from. But I'm not trying to impugn anyone's report.

Q And showing you what's been marked and previously admitted as 12.7A, Page 21, you've reviewed the discovery and seen the passport?

A So I -- you say I've reviewed --

MS. SCANLAN: Objection. Relevance.

THE COURT: That's sustained, Counsel. Let's move on.

BY MR. CHUN

Q As a lawyer, you're aware that, when the government seizes items, they need to first get a search warrant; correct?

A Well, not necessarily. I seized a lot of items without a warrant when I was policing.

Q Is it your testimony that without consent to -- of the individual, the government can just go ahead and look through a computer without a search warrant?

A That's a different question. That's not my testimony. You asked if I could seize items without a warrant. Yes, you can.

Q To search the computer, does the government need a search warrant?

A Yes.

Q And that takes time?

A Yes.

Q And this computer, it was seized in the Maldives?

A I'm sorry -- apparently. That's what I understand from the government's reports, yes.

Q And it traveled to Guam?

A Yes.

Q And then it came to Seattle?

A Same basis for my understanding, from reading the reports, yeah.

Q All of that takes time?

A Yes.

Q Now, you talked about Connected Standby, and you initially said -- or you have said it's to conserve battery; is that right?

A That's correct, yes.

Q You said that's a primary goal of Connected Standby, is to conserve battery.

A I think that's fair. Because you want the computer to be not doing anything but just waiting for wireless signals, yes. And that's the only reason -- why not just have it be totally on all the time? Because it's on battery, preserving battery.

Q And that's why it's not going to be touching this file and that file and creating all these changes, because it's trying to save battery; is that your testimony?

A That's fair, yes.

Q But in Connected Standby, a computer actually can do a lot of things; can't it?

A Yes, it can.

Q It could play music?

A That's not strictly -- from a technical sense, you can -- so in sleep mode is -- the computer is off. It's just a way of preserving the computer, being off. And standby and sleep mode are the same things.

In Connected Standby, you have a timer that allows you to try to connect. You can also set your computer up to run various apps while everything else is turned off, including music. But you will not get the same battery performance, if you play music while in Connected Standby. And it can do other things too. You can have it --

Q So the question was, can it play music while in Connected Standby?

A So the answer is, no. Connected Standby, that's not -- Connected Standby is a specific mode feature. It doesn't -- your question doesn't make sense.

Q Are you saying it's in Connected Standby for 30 seconds, and out of it to check, and then back in it again? Is that what you're saying?

A Right. Yes. And so if it was trying to play music with that being the only thing making it play music, the music would be intermittently on, off, on, off, on, off. That would not work for anyone. So with instructions to the computer, you can say, "Turn everything off, but still play music." But that's not a Connected Standby mode. That is a "computer on" mode, but trying to preserve battery power through other means.

Q You can check e-mail while in Connected Standby?

A Yes.

Q It could apparently receive phone calls, you said?

A Yeah. The checking e-mails, that's the wireless connection, is to see if I'm pushing files, so e-mails, text messages, updates to other apps you have, like WhatsApp, you know, all the social media, Facebook, all that stuff.

Q System updates?

A System updates will not get triggered by Connected Standby, because that drains too much battery power.

Q It can run during Connected --

A If you separately schedule them to run, yes --

Q Yes --

THE COURT: Excuse me. Excuse me. Wait until the question is asked.

And Counsel, wait until the witness has finished answering his question. It's causing total confusion for the court reporter to be able to get it. So please wait.

Ask another question.

MR. CHUN: Yes, Your Honor. I apologize.

BY MR. CHUN

Q Antivirus can run during Connected Standby?

A So I guess I would have to stick to my same answer, which is, Connected Standby is a specific feature of the computer. If you're saying can an antivirus run when the computer is asleep? No. The computer has to wake up to run antivirus. It can be told and scheduled to do so, to wake itself up and run antivirus. But that's not anything to do with this other thing we're talking about, Connected Standby.

Q So when a computer is in Connected Standby, it could repeatedly wake up to do system activities; correct?

A When the computer is asleep, it can repeatedly wake up to do selected activities. Connected Standby is a kind of "unsleep." But it's not -- it's not a mode that can do other things. The computer has to wake up to do the other stuff.

Does that make sense?

Q So when it's in Connected Standby, it can repeatedly wake up, is what your testimony is.

A Actually, the mechanics of it are just, the computer is asleep, but computers have a -- you know, they can keep time. And they do that by having a little battery onboard. So the little watch battery, or what have you, is still running, and it's attached to a timer. And when the timer goes off, the computer wakes up and says, "What" -- "Am I getting e-mail push?" and so forth. That's Connected Standby. It can also have timers for these other things you're talking about.

Q So it could repeatedly wake up out of Connected Standby?

A Yes. A computer can wake up out of Connected Standby, yes.

Q And it could repeatedly wake up to run system activities?

A Yes.

Q To run antivirus?

A If scheduled, yes.

Q To run system updates?

A Again, if it's scheduled, yes. It's not common, because people would be angry if their computer updated itself and drained all the battery power, when they were hoping to have ten more hours.

Q And earlier you testified that everybody was so excited about Windows 8, that it was adopted so quickly; correct?

A I don't think I said it quite that way. But, yes, it was much anticipated, Windows 8.

Q The same operating system that Microsoft dropped in about a year's time; is that right?

A Yes. Anticipation did not match the actual -- you know, the -- how it actually turned out.

Q And earlier you testified that about 3,000 or so files had changed access dates; correct?

A Correct.

Q But of those files, only 274 or so were -- had modified dates that were changed; is that right?

A No. That's -- I mean, they all have -- they all have modified dates that are changed. Even if the modified date is the same expiration date, it's going to have a modified date. So all files have modified dates.

Q Modified dates changed after July 5?

A Oh. Sorry. How many, did you ask?

Q Approximately 274.

A Yes. That sounds right to me, yeah.

Q So not all 3,000 files were showing modified dates that were changed after July 5.

A That's correct.

Q And you've reviewed that list of 3,000 or so files?

A Well, yes.

Q Can you point to any of the government's exhibits on that list?

A I don't know that I know what the government's using for exhibits in this case. My answer is no to that. I don't know what the government's using.

Q And you've testified here that all the evidence on the laptop is unreliable because of these changes; correct?

A Well, my point is that, when you're in computer forensics, you look for suspicious activity. If it can't be explained, you suspect everything, yes.

Q And in your report, you actually give four theories that you believe might have happened; true?

A Four or more theories, yes.

Q Perhaps live imaging went wrong?

A Yes.

Q Perhaps copying from defendant's laptop to another device was done by an agent?

A I don't know who would have done it. I don't know enough about where the computer was. But, yeah, I mean, user-type activity that cause all these access dates to occur. And I gave some of my theories about how that might have happened.

Q Or an agent just logged in and started looking at the computer before it was imaged?

A Yeah.

Q Or that there was network access to this laptop, and that somebody remotely logged in?

A That's right, or pushed files to it, or it automatically grabbed files. All that stuff is not in my report, because I didn't know about the SIM card until after I had written my report.

Q And these were your best reasons for these 3,000 access date changes?

A Well, I would say my favorite reason now would be the SIM card.

Q So your favorite reason is that somebody remotely logged into this computer?

A I think my favorite reason would be that the computer connected to a network and pulled or pushed data in or out, and that changed -- or tried to -- and that changed all these -- or connected to a network, and that's what helped change all these system files. But I don't know. I'm just telling you what I -- if I had to pick a favorite, I think that would be what I would pick now.

Q So let's talk about your theories, the first two, unreliable live imaging or copying of files.

Copying a file would create -- or change access dates; is that right?

A Not if done forensically correctly.

Q Moving a file?

A Same answer. I mean, there are ways to move files without changing the dates, sure.

Q These actions could change the dates.

A They could change dates, but they shouldn't. I mean, it's even -- you don't have to be a computer forensics person. You can XCOPY -- it comes built in with Windows -- move files, and they won't change their dates.

Q Showing you what's been admitted as Government Exhibit 13.5, would either of those theories explain this file just showing up?

A Oh, you mean the miraculous creation theory?

Q It's your theory. I'm asking you, would this -- would the operating system have just created this file?

A I don't think so, no.

Q And looking at the dates of this, this was a receipt for when defendant was in the Maldives, right before he was arrested?

A Honestly, I can't -- I don't disagree with you, but I can't read it very well. But I don't disagree with what you're saying. I just don't -- please don't ask me to say what it says. I can't read any of the words.

Q And showing you Government Exhibit 13.2, which is PACER login records from a cached web page taken off the browser, the operating system wouldn't just create that, based on your two theories; would it?

A No. I don't think any of my theories would cause documents to be created. I should say, any of the theories that you're referring to. That's not what we're talking about.

Q So these cached pages showing Page 2, based on the first two theories, they wouldn't just show up. The operating system wouldn't just make them in that process.

A That's right.

Q And that would be true of 13.12C. Credential -- that's a password login file with defendant's logins and IDs, passwords, Liberty Reserve accounts.

The operating system wouldn't just create those either; would it?

A None of my theories are that the operating system just did anything. I'm talking about user interaction.

Q Going on to user interaction, your third theory was that an agent logged in and just started browsing what was on the computer; correct?

A Yeah, that's right, or trying to do some kind of -- trying to try some passwords out and get through them, you know, some -- yeah, something like that. I don't know. I'm just offering some possibilities.

Q And perusing a computer wouldn't create new files of substance; correct?

A That's right.

Q And so it wouldn't have just created 1.7 million credit card numbers; right?

A That's right.

Q Agents just looking at the computer were contained to that computer; isn't that right?

A That's correct. I will continue to agree with you that none of what you're talking about has anything to do with creating any records on the computer. It was trying to explain why do we see thousands and thousands of access date changes, and then what's next after that.

Q And showing you Exhibit 13.10, credit card log files, that's true for that, as well?

A So -- true; that it doesn't get miraculously created, yes.

Q And that's the same for 13.13, which is a script for the website posdumps?

A Yes.

Q Agents just perusing a computer, if that's your theory, wouldn't have created this.

A Well, I don't know what the agents did or didn't do. But my access date changes that I called attention to, they would not -- unless they're these files, and I don't know, they wouldn't be -- that wouldn't cause these files to appear, no.

Q And you talk a lot about this computer connecting, whether through SIM card or wi-fi; that in Connected Standby, it could just connect to the internet; right?

A That's the definition of Connected Standby, yes.

Q That's your fear, that this computer just connected to the internet?

A That's the fear of anybody who seizes a connected device. That's why we have Faraday enclosures.

Q And that would involve connecting from the Maldives, to Guam, to Seattle; correct?

A I'm sorry. I just don't follow.

Q It would have connected in the Maldives, and it might have connected -- you can answer.

A Oh, that it would try to connect wherever it could connect? Yeah, I think a Connected Standby computer would try to connect wherever it can connect, yes.

Q And then try to connect in Guam?

A Yeah. I think anywhere it's on, in Connected Standby, by definition, it's going to check and see if it has wireless connection capability. Whether it could connect or not, I don't know.

Q And if the laptop is changing networks that it's on, it's also changing its connecting IP address; correct?

A Normally, yes.

Q A wi-fi network in the Maldives would have a different address than the one in Guam; yes?

A I'm not -- I think you're generally right. Of course, you could get a hard IP that traveled around with the machine. But I think what you're saying is a fair guess, yes.

Q And it would be different, again, in Seattle?

A I would think so, yeah.

Q And finding one computer in the world is very different from scanning open ports on the internet; correct?

A I don't understand that question.

Q Finding -- the task of finding one individual computer, somewhere in the world, is a different task from port scanning open -- looking for open ports on the internet.

A Those sound different to me. So, yes, I agree.

Q Are you familiar with what "port scanning" is?

A Yes.

Q Are you familiar that it's just pinging out into the internet, checking for ports at different computers or networks?

A That's not what port scanning is. Port scanning is interrogating a computer and asking it what ports it has and what their status is. If you're using it for nefarious purposes, maybe you're port scanning times 10,000. But port scanning is used every day by network administrators.

Q And that task is very different from finding one computer somewhere in the world.

A What do you mean by "finding one computer somewhere"? That's the part I don't get.

Q Your fear of this defendant's laptop is that somebody remotely pushed files onto it and caused changes; right?

A Yeah. That would be the reliability fear, yeah. That's -- all my training is, don't let it connect, because changes might occur, either out or in. Yeah.

But by that same connection, what you're saying doesn't make any sense. I mean, the computer could just as easily, through all these scheduled things we've been talking about, announce its location and availability. And that's also very common in networks. In other words, the computer connects and says, "Okay. Here I am. Push me data." So you don't -- it's not hard to find. That's not the challenge. Otherwise, we'd never worry about that in any forensics case. And we worry about it in every forensics case.

Q And SIM card aside, talking about wi-fi, when you say "connecting to open wi-fi," you mean something without a password.

A Yeah, I think that it's -- in my opinion, and there might be someone who would disagree with me -- I think that the default settings are going to be always: You're only going to connect to either open or trusted networks, and you're not going to try to bust into an unknown, non-open network, that you don't have a password to.

Q And so that would exclude places like coffee shops that have the password "Island Coffee"?

A That would -- yeah, that would not be an open network, so that would exclude any non-open network, yes.

Q And it would exclude a hotel that makes you agree to terms and services?

A I don't -- I just can't answer. I don't know. It would exclude any network that was not open, any wandering wi-fi thing you can't connect to. I totally agree with that. We've all experienced that.

Q It needs a completely unprotected wireless network.

A Well, it needs either a network -- on the wireless only. We're not talking the SIM side -- either a wireless network that it has connected to before, because it knows it will reconnect, or it needs an open network. I don't think that -- "open" and "unprotected" are not the same, but just "open" meaning not password protected.

Q And so your fourth theory about this computer was remotely accessed by someone, you're stating that they planted evidence on it?

A No, I'm not saying that.

Q Now, your theory is that this computer remotely connected, whether through SIM card or wi-fi. That's your fear; correct?

A Well, I mean, I guess you're using those two things interchangeably. It's my fear. I don't think it's my theory.

I don't know what happened to this computer. The reason I give so many examples of issues that could have happened with the computer is because I don't know. And therefore, in my opinion, the evidence is unreliable. So the "fear" part, I agree with you. But this theory that, or this theory that, I don't know. I'm only working with the data the government gave me.

Q Isn't that what a theory is?

A A fear?

Q A theory is.

A I'm -- I'm saying you're asking me a question where you're saying the theory and the fear, as if they mean the same thing. And to me, they mean two different things.

THE COURT: Members of the jury, if you'd like to stretch, please feel free to do so.

BY MR. CHUN

Q Handing you -- do you recognize that?

A I do.

Q What is it?

A This is a report I created March 1 of this year, about my analysis of the laptop.

MS. SCANLAN: Do we have an exhibit number for this?

MR. CHUN: And, Your Honor, the government would like to mark this as Government Exhibit 22.

THE COURT: All right. Please continue.

BY MR. CHUN

Q Mr. Blank, is that your report of your forensic examination of defendant's laptop?

A Yes, it is. Yes, it is, to that point. I mean, I did some more work later. But, yes, up to March 1, yes.

Q That's where you put forth your -- the possibilities that the agent logged in, or a hacker, or a remote connection occurred? Is that that report?

A Yes. That's where I was trying to come up with my explanation for the thousands and thousands of access dates and some of the possibilities associated with that, yes.

Q Now, could you tell me the page number in your report where you examine the forensic artifacts for last network connection?

A Is that in my report?

Q That's what I'm asking you.

A Oh, no. I think all of that work occurred afterwards.

Q So in writing your report, a theory that somebody may have logged into this computer, you didn't actually look to see what the network connections showed?

A I have looked at the network connections. And honestly, I don't remember if I looked at them before or after this report. So I don't know.

Q So you wrote the report without ever even looking at it on the computer; is that your testimony?

A Well, I think I made these possibilities. And then I was asked to continue working in order to determine whether or not I could rule in or rule out these possibilities. That's when I would look at all these logs, and so forth.

Q So you wrote the report about these theories without ever even looking for the forensic artifacts on the laptop?

A I think that's -- when you say "without ever," I mean, so it's clear, that I did explore these theories later. But did I do this report on, I think, about -- I mean, I think I went through this at the hearing. I have a very good reason for that. So, yeah, you are correct. I had a very good reason for that.

Q So your answer now is, you wrote this report about this laptop without looking at the forensic artifacts for network connections on the laptop.

A And my answer is, that is correct, and I had a very good reason for that.

Q And the computer does have numerous places where it would log the last connection; right?

A One hopes. They're not infallible; but, yes.

Q And as we talk about your report, on the last page, is that your signature?

A Yes.

Q And so you made these conclusions about the laptop without even looking at the forensics on the laptop.

A Well --

MS. SCANLAN: Objection. Asked and answered.

THE COURT: That's sustained, Counsel.

THE WITNESS: Ask me.

THE COURT: Sir, there's no question before you. Next question?

MR. CHUN: Yes, Your Honor.

BY MR. CHUN

Q And you're aware that the network profile registry key within the software registry hive shows the last connection?

A Yes.

MR. CHUN: I apologize, Your Honor. May I approach, Your Honor?

THE COURT: You may.

MR. BROWNE: Counsel, are those exhibit numbers?

MR. CHUN: It appears the paralegal labeled each one for a specific person.

BY MR. CHUN

Q Showing you what's been marked as Exhibit 18.1, isn't that the network profile registry key from defendant's laptop?

A Sorry. In the book or on the screen?

Q Either/or. And that would be a two-page exhibit.

A I see it.

THE COURT: Counsel, is there a question?

MR. CHUN: Yes, Your Honor. I'll repeat it.

BY MR. CHUN

Q Is that the network registry key within the software registry hive from the defendant's laptop?

A I believe so, yes.

MR. CHUN: Your Honor, the United States moves to admit Exhibit 18.1.

THE COURT: Any objection?

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Blank, did you create this exhibit?

A I did not.

Q Do you know, then, whether this is actually the network registry key for that laptop?

A No, I don't. I'm just trying to be cooperative.

MS. SCANLAN: I would object to the admission of this exhibit through this witness.

THE COURT: Sustained, Counsel.

Next question?

CROSS EXAMINATION

BY MR. CHUN

Q Earlier you testified, after writing your report, you went back and looked at the forensics on the computer; correct?

A Well, I don't think it's fair to say I didn't do any looking at forensics on the computer. You asked me did I look at logs at the time of the report. I told you that I had not, for a good reason. Those, I did look at later, yes.

Q Do you recognize this log?

A Well --

MS. SCANLAN: I'm going to object. This has not been admitted. It doesn't appear that it's going to be.

THE COURT: The Court hasn't made that determination, Counsel. He's inquiring as to whether or not he had made a subsequent determination in later reviewing.

So that objection is overruled. The witness is permitted to answer the question.

THE WITNESS: I don't -- I don't -- I don't think that it's not. But I do about five computers a month, and I can't tell. I can't tell you. I don't doubt what you're saying, but I can't say that I recognize it. I don't recognize it and -- I just don't. I can't say any more than that.

BY MR. CHUN

Q Showing you 18.2, is that the network profile operation event log from the defendant's laptop?

A My answer would be the same. I mean, I don't doubt what you're telling me, but how -- I don't know.

Q And the network profile operation event log would log the last network; correct?

A Not necessarily. They're not infallible. They may be instructed not to log it. Sometimes computers want to forget the network, because they don't want to connect automatically, so they'll change the network log so that it forgets the login that's normally done. So the answer is, no.

Q Showing you 18.3, isn't that the WLAN autoconfig operational event log from the defendant's laptop?

A I mean, you tell me. So I want to -- I'm giving you the same answer, which is, I don't doubt what you're telling me, but I don't know. There's not enough information on here for me to tell that, one way or another.

Q Mr. Blank, did you review evidence before testifying -- or before coming to testify here today?

A No. Well, that's actually -- of course, I did, but not recently, if that's what you mean.

Q And you didn't review the forensic artifacts on the defendant's laptop?

A Not since our hearing in June.

Q And showing you what's already been admitted, Exhibit 13.47, do you recognize that as the software registry hive key for cellular connections?

A It doesn't look like that to me.

Am I looking at the right one?

Q Could you just go ahead and read what it says, on the right side?

A Yeah. This is not a format that I look at this stuff in. That says, type: "Reg_SZ"; and the data: "MegaFon RUS."

Q And do you see the date that it says it was last connected?

A I do.

Q And what would that date be?

A Tuesday, 17 June 2014.

Q And that's before the defendant was arrested; correct?

A That's my understanding, yes.

Q Now, going back to that March 1 report that you wrote, could you please show me the forensic artifacts you listed in there for the last time a person logged into the computer?

A So, I mean, relying on that information from the wireless log? That's not referenced in this report, for a good reason.

Q Does your March 1 report indicate any forensic artifacts showing the last time a user logged on to it?

A I don't believe so, no.

Q It doesn't list any?

A I'm sorry?

Q It doesn't list any artifacts?

A Showing login, I don't think so.

Q But a computer does keep track of that; correct?

A A computer does keep all kinds of logs, yes.

Q And you didn't think it was important to put that in your report?

A I think it was very important to put in my report. I think it's something that should go in every report, whenever possible. And so -- that's my answer.

Q If you could flip to Government Exhibit 18.6.

A Okay. I'm there.

MR. CHUN: One moment, Your Honor. I apologize.

BY MR. CHUN

Q Moving on from that exhibit, showing you what's been marked as Government Exhibit 18.11, do you recognize that as a system resource user manual from the defendant's laptop?

A No. I've never seen this document before, in paper.

Q So you've never seen the SRUM logging activity from defendant's laptop?

A I've never seen the SRUM in paper. I've looked at it on the screen, but I didn't -- I'm kind of a paper conserver, and I didn't print it out. So I don't recognize the document. And that's my answer.

Q Does the paper record the activities indicated on the screen that you saw it on?

A The SRUM log is kept in a different format. If this is

SRUM data, and I have no reason to doubt that it is, someone has very nicely compressed it and put it into a nice format, where it fits on the pages, which is a nice thing to do, but it means it looks different than a SRUM log that I would see.

Q And earlier you had testified that you had spent about 250 hours on this case?

A Yes.

MR. CHUN: No further questions, Your Honor.

THE COURT: Redirect?

REDIRECT EXAMINATION

BY MS. SCANLAN

Q You were asked some questions about how long it takes to get a search warrant; do you recall that?

A Yes.

Q Have you ever gotten a search warrant in less than 23 days?

A Yes.

Q Have you ever gotten a search warrant in less than two hours?

A Yeah. There's always somebody on call. You wake some poor judge up at 2:00 in the morning, and get a search warrant in 30 minutes.

Q And then there was a lot of questions about whether this system -- the operating system would create certain files; do you recall that?

A Yes.

Q So we looked at some examples of that, right, up on the screen, different files, and then there was questions about whether the operating system could create those files?

A Right.

Q Are you saying somewhere that this computer operating system created these files?

A No, I'm not saying that.

Q And is an operating system creating a file the same as a file being sent to a computer?

A No.

Q Is it possible that a computer that is not protected in a Faraday enclosure, and has this radio connectivity, wireless connectivity, is receiving files?

A Of course; or file changes to the files already on there, or sending files off, and all that kind of activity. When we receive an e-mail, we don't say the operating system created the e-mail. We say it received it through a wireless connection.

Q But to be clear, are you saying that that definitely happened in this case?

A No, I'm not. I don't -- I don't know what definitely happened. My focus has been, okay, from a computer forensics standpoint, we have rules. And the rules were broken here. Don't trust this data, because all kinds of things could have happened. And I stand with the -- you know, the head of the FBI, saying, "Look, under these circumstances, you can't tell whether something has happened or not." And that's -- I think he's totally right. I agree with him. I think the computer forensics world agrees with him. And so I consider this to be unreliable.

Q Was the SIM card on this computer discovered by the Secret Service, with the arrow, before or after you wrote your report?

A After.

Q Did you start looking into the possibility of that radio network connection before or after the Secret Service found the SIM card with the arrow?

A I just -- I don't remember. I remember it being, like, one of the possibilities that was discussed, but I don't remember.

Q So you were asked questions about different logs, and SRUM journals, and that kind of thing; do you remember that?

A Yes. I'm sorry. I just remembered that.

So the -- no, the SIM -- the whole SIM issue was a big deal from the beginning. Because this computer, when it came out, that was kind of touted, this whole Connected Standby, use it for stuff. So the possibility of SIM was a concern from the beginning. So I'm going to change my last answer.

Q Okay. So the SIM card was a concern from the beginning.

But to your knowledge, in March of 2016, when you wrote this report, did you know that this computer had a SIM card?

A No.

Q And had you examined the actual computer at that point, in March?

A Yes, I -- I had not examined the actual computer at that point, no.

Q Do you have the computer there now?

A I think so. I mean -- I don't mean to be difficult. Again, a computer was handed to me. I guess I'm just believing it's the computer.

Q Have you got that exhibit -- Exhibit 12.8, do you have that, in your hands?

A Yes.

Q Are you looking for the exhibit sticker?

A No, just looking at it.

Q Is that the first time that you've actually handled that computer?

A Yes. Sorry. I'm sorry. Go ahead.

Q So the -- we had all these -- moving on to the logs; okay?

A Yes.

Q You were asked questions about different logs and this journal thing, and whether there was information in it; right?

A Yes.

Q And when you saw on this exhibit -- did you see on the exhibit when they were pointing out the last connection was

June 17; do you recall that?

A Right -- okay. Yes, is that -- I'm not sure that's the right date. But, yes, the -- yes.

The one with the MegaFon on it?

Q Right. Was the connection date before the laptop was seized?

A It's kind of a giveaway that there was a SIM card, the fact that the connection refers to a telecom company.

Sorry. What was the question?

Q Was that connection date before it was seized on July 5?

A Yes.

Q That log that you were looking at -- and we've talked about this before, but I just want to be clear with that specific example -- is that something that can't be changed?

A Oh, it can absolutely be changed. It is, in many ways, as difficult to change as a Word document, or WordPad, or, you know, notebook-type document. It is just lines of plain text that you can edit to your heart's content with an editor tool, and editor tools are widely available. And it's done for -- it's not just hackers that have these things. It is done for legitimate reasons, for administrative purposes.

Q So the fact that that exhibit shows the last connection date before July 5, does that tell you that this information on this computer is reliable?

A No. The -- absolutely not. So does that mean that I should say, "Okay. Well, therefore, no more investigation is necessary, because, look, a log says the last connection was prior to July 5"? That would be terrible work on my part. Absolutely, that does not change the reliability question.

In fact, given that it has Connected Standby, it has a SIM card, you have to wonder why is that the last connection? I mean, it really last connected weeks before July 5? That's odd. So it makes me question the log even more.

MS. SCANLAN: I have nothing further, Your Honor.

THE COURT: Further cross?

MR. CHUN: Yes, Your Honor.

THE COURT: How much do you have, Counsel?

MR. CHUN: Maybe about five minutes, Your Honor.

THE COURT: All right. Let's go ahead and finish this witness.

MR. CHUN: Yes, Your Honor.

RE-CROSS EXAMINATION

BY MR. CHUN

Q Just to be clear, you're not saying that the director of the FBI told you that the forensics of this laptop were unreliable; right?

A He was speaking of another computer, correct.

Q And even though you didn't know this laptop had a SIM card, you knew it had wi-fi; yes?

A Yes. You can't have Connected Standby without a way to be connected.

Q So there was still a reason to look for network connections?

A Yeah. And I did.

Q Did you ever ask to come and look at the laptop?

A Yes, I did. I wanted to run a bunch of hardware tests on it.

Q And another individual with the defense team came and looked at it; correct?

A That's my understanding, yes. But to be clear, not anyone from my shop.

Q You can alter access dates also; true?

A Yes. And, in fact, a lot of programs that we use every day actually do change the access dates. They just change them back, at the end, so that it looks unchanged. But the actual mechanism is access date gets changed, something happens, access date gets changed back.

Q You can purposefully alter those, also.

A Yeah, that's true.

Q And so what you're saying is that the log files could have been altered.

A Yeah. Of course they can, yes.

Q The few log files that connect to -- that show wi-fi connections.

A Yeah, I think they absolutely could be, yes.

Q And same with the SIM card?

A What do you mean by that? The SIM card --

Q The log with the SIM card, that would indicate the use of a SIM card.

A Yeah. I think that shows up on this computer as part of the wireless connection log.

Q So you believe somebody could have gone back and altered those, but wouldn't have bothered with 3,000 access dates?

A That's the trick in computer forensics. If you catch one little mistake, because people aren't perfect about making changes, then it makes -- and that's exactly -- you've just told me the reason why we have all these protections in computer forensics, because people do try to change stuff all the time. And you only get little pieces of clues that it's been changed. And that's why, then, okay, what else was changed? Who knows? Because they could have gone and done a lot of other stuff. You just don't know. So that's why, when you find unexplained, suspicious items, you have to mistrust the whole thing. And that is really lesson number one in computer forensics.

Q And the 3,000, they would have missed; but the few, they didn't?

A Well, how do you know it's a few?

Q The few log files.

A Oh, if you're just going to change log files, there are routines that you can just -- that will address just log files. So that could just be one project, really, is to change log files, if that's what you want to do.

Q And isn't it true that the last time the MegaFon network was connected to was in June, is possibly because that was the last time it was connected to?

A But my testimony is that, in my opinion, I don't trust or rely on that log file that you're referring to. So I don't agree that we can agree that that was the last connection.

MR. CHUN: No further questions, Your Honor.

THE COURT: Further redirect?

MS. SCANLAN: No, Your Honor.

THE COURT: Any objection to this witness being excused, on behalf of the defense?

MS. SCANLAN: Yes.

THE COURT: You are objecting?

MS. SCANLAN: I am.

THE COURT: You're not excused, sir. You may be subject to recall.

Members of the jury, we'll take our afternoon recess. And to make sure that you have a full afternoon recess, we'll resume at 1:40 this afternoon. Have a good lunch.

(Jury exits the courtroom)

THE COURT: Please be seated.

Counsel for the defense, what's the next step for your case?

MS. SCANLAN: Your Honor, the defense will rest.

THE COURT: And, Counsel, I just want to inquire to ensure the defendant understands that he has a constitutional right to testify.

Mr. Seleznev, I want this to be interpreted. I know that you waived the opportunity for some portion, significant portion of the trial, but I want to make sure you understand, so the interpreter is going to be doing a word-for-word translation.

Sir, I want to make sure that you understand that at this point in the case you have the right to testify.

Do you understand that, sir?

THE DEFENDANT: I understand.

THE COURT: And have you had the opportunity to consult with counsel regarding your right to testify in this case?

THE DEFENDANT: Yes, I did.

THE COURT: And based upon your communication with your lawyers, is it your desire that you wish to waive your right to testify in this case?

MR. BROWNE: I think the word "waiver" is -- may I just --

THE COURT: Certainly.

MR. BROWNE: Your Honor, may I -- we've had this discussion numerous times with my client. And I think he's choosing not to testify. He knows he has an opportunity to.

THE COURT: I'll rephrase it, Mr. Seleznev. Disregard the last question about waiving.

You have the opportunity to testify in your case.

Do you understand that?

THE DEFENDANT: Yes, I do.

THE COURT: And you understand that you would have the right to get on the witness stand, be placed under oath, the same as all the other witnesses, and provide testimony on your own behalf.

Do you understand that, sir?

THE DEFENDANT: Yes, I do.

THE COURT: And have you discussed your right to testify in this case with your lawyers?

THE DEFENDANT: Yes, I have.

THE COURT: And have you elected not to testify in this case, after conferring with your lawyers?

THE DEFENDANT: Yes, I have.

THE COURT: Is anyone forcing you to make that decision?

THE DEFENDANT: No.

THE COURT: Is that a decision that you reached based upon your own conclusion that you wish not to testify?

THE DEFENDANT: Yes.

THE COURT: So no one's pressuring you in any way?

THE DEFENDANT: No. No one is pressuring me.

THE COURT: Has anyone promised you anything if you don't testify?

THE DEFENDANT: No.

THE COURT: Counsel, are you aware of any reason why the Court should not make a determination that your client is knowingly, intelligently, and voluntarily waiving his right not to testify in this case?

MR. BROWNE: No, Your Honor.

THE COURT: All right. Counsel, the defense will necessarily have to rest their case in front of the jury, obviously, after lunch.

And counsel for the government, will you be putting on rebuttal testimony?

MR. BARBOSA: Yes, we will, Your Honor.

THE COURT: And the witness that will be providing rebuttal testimony?

MR. BARBOSA: Ovie Carroll.

THE COURT: Then if nothing further, anything to bring up, by the defense?

MR. BROWNE: No, Your Honor.

THE COURT: By the government?

MR. BARBOSA: No, Your Honor.

THE COURT: We'll be in recess. We'll see you at

1:40 this afternoon.

(Recess)

(Jury enters the courtroom)

THE COURT: Counsel for the defense?

MR. BROWNE: Yes, Your Honor. The defense rests.

THE COURT: Counsel for the government, any rebuttal evidence or testimony?

MR. CHUN: Yes, Your Honor. The United States calls Ovie Carroll.

THE COURT: Please have him step forward.

THE CLERK: Please raise your right hand.

OVIE CARROLL, having been duly sworn, was examined and testified as follows:

THE CLERK: If you could please state your first and last names, and spell both for the record.

THE WITNESS: First name is Ovie, O-V-I-E, and the last name is Carroll, C-A-R-R-O-L-L.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MR. CHUN

Q Mr. Carroll, how are you employed?

A Currently the senior executive for the Department of Justice, in charge of the cybercrime lab.

Q And how long have you held that position?

A Ten years and eight months.

Q And what do you do in that position?

A I'm in charge of the Department's cybercrime lab that consults with all prosecutors across the country on high-level, high-technology cases.

Q And what did you do before that?

A Before that, I was a special agent in charge of the Technical Crimes Unit for the Postal Inspector General's Office. And there we did all the intrusion cases, computer hacking, any high-level computer forensics. And then I was also in charge of the technical services section, which was the body wires and covert cameras.

Q And how long were you there for?

A Five years.

Q And before that?

A Before that, I was special agent in charge of the Air Force Office of Special Investigations, Washington Field Office, where we did all the computer hacking or computer intrusion cases across the world that affected any Department of Defense or Air Force matters.

Q And in your current role, you just said you were a senior executive; is that right?

A That's correct.

Q What does that mean?

A Well, that's -- my pay grade is senior executive, and I'm the senior adviser to Department of Justice officials. When the Attorney General or Deputy Attorney General have a high-technology case, and they need to understand the technology, or have a question about it, I'm their senior adviser inside the Department of Justice.

Q What training have you received to become a forensic examiner?

A I started 20-plus years ago in the Air Force. They were standing up the first-ever computer forensics operations for any federal law enforcement agency. And I had done some computer work that they felt I was skilled to do it, and they asked me to be one of the first people to stand up this agency.

Q And, I guess, over your career, have you received other training?

A Yes. I receive training yearly from a number of places, to include vendor training, the SANS Institute, any of the computer forensics training courses that are out there.

Q And do you teach any computer forensic courses, yourself?

A I do. I teach computer forensic courses, both inside the Department of Justice, as well as outside. On the outside, on a part-time basis, I'm an adjunct professor for the past eight years with George Washington University, where I teach in their master's program for high-technology crime. I also am a certified instructor and a coauthor for the SANS Institute for a course called Advanced Windows Forensics Investigations.

Q Sorry. What is the SANS Institute?

A The SANS Institute is a training organization that teaches internationally all types of computer courses. They started years ago with security audit networking. And over the past 15 or so years, they've expanded -- or 20 years, they've expanded into computer forensics, hacking, WIPAC, penetration testing, all types of computer-related courses.

Q Are you a part of any professional organizations?

A I am. I am the -- on the federal advisory board for the Organization of Scientific Area Committees. I'm the task chair, the task group chairman, for the Digital Evidence Committee. I'm also on the Scientific Working Group on Digital Evidence Committee.

Q And do you have any role with vendors of forensic tools?

A I do. I am one of -- on several federal advisory boards for the large forensic tool software vendors, such as AccessData, Magnet Forensics, et cetera. And they routinely will come to me, or bring me in, and show me new developments that they're doing on their tools, ask what it is that the community needs, where they can improve their product, et cetera. And this is an unpaid role.

Q What tools does AccessData make?

A They make several, but their primary tool is a tool called FTK. It stands for Forensics Toolkit. That's one of the two primary tools in the forensics community. They also make FTK Imager. They have network monitoring tools and appliances that they can put out there for intrusions. They have mobile forensics. They have a number of tools.

Q Now, in your career as a forensic examiner, how many computers have you reviewed?

A Hundreds or thousands in the last 20-plus years.

Q And how many of those ran a Microsoft Windows operating system?

A I'd say in the mid-'90s, I think 90 percent of what we see in the lab, over the last 20 years, have been some variant of Windows, from Windows XP up through Windows 10. We're starting to see more Macs now. But predominantly, it's been Windows.

Q Would that include Windows 8?

A Yes.

Q And variations of Windows 8?

A Absolutely.

Q And that would include 8.1 or professional versions of 8 or 8.1?

A Both the consumer versions, as well as the professional versions of Windows XP, Windows 8, 8.1, and 10.

Q Do you also teach classes on Windows 8 or variations of it?

A I do. I teach that for both the Department of Justice, as well as the SANS Institute and George Washington University.

Q Did you review an image of defendant's laptop hard drive in this case?

A I did.

Q And do you have, in your training and experience, an opinion as to whether or not this -- someone would have remotely logged into this computer after it was seized on July 5?

A I do have an opinion on that.

Q What would that be?

A There's no possibility that that happened.

Q And how did you come to that opinion?

A Well, by conducting an exam on the computer, Windows computers, among other things, it records every network that you ever connect to, when was the first time and when was the last time. And it has a number of different artifacts that record what networks you connected to, sometimes the serial number or the Mac address of the network that you received your internet connection from. And I reviewed all of the evidence on the computer relating to what networks have been connected to, and when, and this computer was not connected to any network of any kind after July 5.

Q Showing you what's been marked as Government Exhibit 18.1. You have a binder up there, as well, if that's easier.

A Okay.

Q Do you recognize that?

A I do.

Q What is it?

A It's a screenshot that I took.

Q You created this yourself?

A I did.

Q Is it an accurate representation of the screenshot you took?

A Yes, it is.

MR. CHUN: United States moves to admit 18.1.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, this is a screenshot you took of what?

A This is a screenshot that I took of the software registry hive that came from the image of the defendant's computer.

MS. SCANLAN: I have no objection.

THE COURT: 18.1 is admitted.

(Exhibit 18.1 was admitted)

DIRECT EXAMINATION

BY MR. CHUN

Q Could you tell us, please, what we are looking at here? I'm going to highlight that.

A Sure. So this is the network profiles registry key. So this is one of the forensic artifacts that tracks all the networks that this computer ever connects to, when is the first time it connected; when was the last time it connected, and how it connected; did somebody plug in a network cable, or did they connect over wireless network, et cetera.

Q Could you tell us what the name of the last network was called?

A Yes. The name of the last network was the Kanifushi. You see it highlighted here in blue. Kanifushi was the last network it was connected to.

Q And going to Page 2 of the same exhibit, what are we looking at here?

A As you zoom in there, what you'll see is -- I'll let it refresh. There we go. This, right here, is a 128-bit system structure. So this is a date, time, second, and millisecond of the very first time that this computer ever connected to the Kanifushi network. And then the next line, the very last line, is the very last time that this computer connected to the Kanifushi network.

And what I did is, we have these programs -- this is a program called DateDecode. And this, right here, you'll see that this shows the first time that that computer ever connected. You copy that 128-bit system structure, and that shows you the first time that this system ever connected to the Kanifushi network.

Q And what date is that?

A That was June 21, 2014, at 20:47.

Q And what would be the next date shown there?

A The next date is the last time it connected. And you can see that the last time this computer connected to the Kanifushi network was July 3, 2014, at 21:55.

Q And can you tell what type of connection it was connected by?

A Yes. This, right here, you'll see, is a "NameType" value. And this NameType value, right here, of 47, the hex value 47, numerically 71, says that it connected over 802.11, or wireless.

Q So would that have shown something different had it been a -- plugged in by a cable?

A Sure. If this would have plugged in through a network cable onto the computer, that number would be 6. So each way that you connect to the internet, it has a different value.

Q Would it have -- showing you what's previously been admitted as 13.47, could you explain to us what we're seeing here?

A This is just another one of the network profiles registry keys. And this shows a different network. The network name is MegaFon RUS, as you can see right here. And this shows the first and then the last time that this computer connected to the MegaFon RUS network, and how it connected.

Q And looking at this, can you tell what type of connection it was?

A Yes. As you can see right here, this shows 243, or hex value F3, which shows that it was a cellular, or 3G/4G network connection.

Q And going to Page 2 of the same exhibit, what do we see on Page 2?

A This is the network profiles operational event log. So Windows keeps a number of event logs, and this one records the networks, just another artifact that's duplicative of what we just saw. And it records every time you connect to a network.

Q And showing you Page 3 of the same exhibit, what do we see here?

A This is an event log. We call it Event ID 10001, which shows this is the last time that it disconnected -- that this computer disconnected from the MegaFon RUS network. So this is showing it successfully disconnected.

Q And also showing you previously admitted Exhibit 12.9A, and this being a travel record for the defendant, could you just compare the dates here for the jury, please?

A The dates -- okay. Thank you.

So the date here is listed as June 18, 2014.

Q And looking at Exhibit 12.9A, when did the defendant leave Russia?

A It appears June 16. Or I'm sorry, June 21. There we go. The e-mail was on June 16.

Q Now showing you what's been marked as Government Exhibit 18.2, do you recognize that?

A I do. It's a screenshot of an event log that I captured.

Q Is that an accurate copy of the screenshot you captured?

A It is.

MR. CHUN: United States moves to admit 18.2, Your Honor.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, this is a screenshot you captured of an event log from what?

A From the defendant's image of his computer.

MS. SCANLAN: No objection.

THE COURT: 18.2 is admitted.

(Exhibit 18.2 was admitted)

DIRECT EXAMINATION

BY MR. CHUN

Q What are we looking at here?

A Here, we're looking at the Windows network profile operational event log. And Event ID 10000 represents when this computer connected to a network. And this is showing it connected to the Kanifushi network on June 27, at 11:26 a.m.

Q And the name of that network, again?

A The Kanifushi network.

Q And showing you what's been marked as Government

Exhibit 18.3, do you recognize that?

A I do. It's another screenshot that I took of the event logs from the defendant's computer.

Q Is that a fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit Exhibit 18.3.

MS. SCANLAN: No objection.

THE COURT: 18.3 is admitted.

(Exhibit 18.3 was admitted)

BY MR. CHUN

Q Mr. Carroll, could you please explain what we're seeing here?

A Sure. This, right here, is an Event ID 10001, which shows when this computer disconnected from the Kanifushi network. So you can see on 7/5, recorded at 5:37 p.m., that this computer disconnected from the Kanifushi network.

Q And was that the last connection, or was there a subsequent connection?

A No, that was the last connection of this computer.

Q And showing you what's been marked as Government Exhibit 18.4, do you recognize that?

A I do. It's another screenshot of an event log that I took from the defendant's computer.

Q Fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.4.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 18.4 was admitted)

BY MR. CHUN

Q Now, what are we looking at here?

A This is just another event log. Windows has 60-plus event logs. This particular event log is for the wireless LAN operational. So this only has to do with networks that you connect to wirelessly. And this event log, 8003, shows that the computer had successfully disconnected from the Kanifushi network. And that was recorded on July 5, at 5:37 p.m.

Q We've now looked at several logs.

Based on these logs we've looked at so far, what would be your opinion of whether or not this computer connected to any networks after July 5?

A There's clear evidence that this computer did not connect to any network after July 5.

Q Showing you what's been marked as Exhibit 18.5, do you recognize this? And this is a multipage exhibit, if you want to flip through it in the binder, please.

A I do. This is another screenshot that I took of the defendant's computer. And specifically what we're looking at is the Windows update log.

Q Is this a fair and accurate copy of the log you --

screenshot you took?

A It is.

MR. CHUN: United States moves to admit Exhibit 18.5.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, do you see the red highlighting boxes on this exhibit?

A I do. Here at the bottom?

Q There's one on the bottom of Page 1, and there's some just sort of throughout this document?

A Yes, ma'am.

Q Did you add those to the screenshot?

A I did.

MS. SCANLAN: With that noted, I have no objection.

THE COURT: 18.5 is admitted.

(Exhibit 18.5 was admitted)

MR. CHUN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. CHUN

Q Mr. Carroll, could you please tell us what we're looking at here, in highlight at the bottom?

A Sure. As I mentioned, this is the Windows update log. And Windows -- anytime that you're running Microsoft Windows, it's routinely reaching out to Microsoft to see if there are any updates that your computer needs. And this is the log that tracks -- every time it reaches out to Microsoft to try to see if there are any updates, it records the state of the computer and whether or not it was successful in reaching Microsoft.

Q Looking at Page 2 of this exhibit, you have marked it with a red box.

Could you please explain what we see here?

A Sure. I drew this red box around it to draw attention, for the prosecutor, that this is the last instance in which this computer reached out to check for updates with Microsoft and had a network connection. What you'll see right here is, it says the network state is "connected." And that was all, as you can see right here, on July 5. And this is a multipage log. And I looked through the entire log, and this is the very last time that this computer had any network connection to reach out to Microsoft. All the subsequent entries in this log shows that it reached out, and it did not have a network connection; that the network state was disconnected.

Q And turning to Page 3, what is the -- what have you indicated there?

A This red box here just indicates that, when it reached out at 21:37, on July 5, that the network state was disconnected. And again, throughout the rest of this log, every instance that it tried to reach out to Microsoft, it recorded that it had no network connection.

Q And going to the last page of that exhibit, what do we see there?

A This is just the last entry in that log, saying that the network connection was not detected. Again, it tried to reach out to Microsoft to see if there were any updates, and it just has no network connection.

Q And so looking at the first log, on July 5, and then all the way to the end, what does that tell you? What does that exhibit tell you about the network connection?

A Well, it just corroborates all the other forensic artifacts that said this computer had no connection to the internet after July 5.

Q And that would be true to the end of the date that was recorded?

A Correct.

Q And were there any logs after that?

A After July 5?

Q No, after the last page of the exhibit we just saw.

A No. That was the last log of that particular Windows update log.

Q Showing you what's been marked as Government Exhibit 18.6, do you recognize that?

A I do. It's a screenshot that I took from the defendant's computer.

Q Fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.6, Your Honor.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 18.6 was admitted)

BY MR. CHUN

Q And what are we looking at here?

A This is an interesting log that Microsoft created in Windows -- started using in Windows 8. And it's called the system resource usage monitor. And what it's doing, it's primarily designed for diagnostic purposes. And it's recording -- what you're seeing here is every application on this computer that's running and who's responsible, what user is responsible. This is the user that's responsible for running that application. And then it shows here how it connected to the internet. And in this case, 802.11 is our wireless connection. And it tells what wireless network it was connected to, which is the Kanifushi. And then for each application, it shows how much data came into the computer and how much data left the computer.

Q And what does the last -- last line of activity here on this report tell you about the computer's connection to a network?

A The last network that it connected to, again, was the Kanifushi network. And it shows no connectivity after July 5.

Q And the second page of this exhibit, what are we looking at here?

A This is the -- another table in that database called the system resource usage monitor. And this one is specifically the network connectivity database. And this, again, shows the network that this computer was connected to, anytime it was connected to a network. And when that network connection started is this last line; and then the connection time, how long it was connected to that particular network.

Q And what is the date and time of the very last connection there?

A The last connection is, again, on July 5, 2014, at 17:38.

Q And comparing that to the second page of Exhibit 18.1, what do we see how the times compare? We'll zoom out in a second.

A Okay. So this shows that the last time that this network connection was established was July 5, at 17:55. And if you go to the other exhibit, remember I told you that this entry is also the last time. And here, you see that the last time was 21:55. This is the difference between local time versus UTC, or Greenwich Mean Time. So this shows that both had the exact same time, further just corroborates -- the nice thing about Windows is, it records in multiple locations things that happen.

Q Do you know what "Connected Standby" is?

A I do.

Q What is it?

A Connected Standby is a feature that was introduced in Windows 8. And it's really a software, but predominantly a hardware feature. It's on very few computers, right now, because the computer itself has to actually have particular components installed. For instance, it has to have a low-power RAM, DRAM. This is the upper memory of the computer. It typically has to have a solid-state hard drive in Windows 8 or 8.1. And it also has to have what they call "system-on-chip," so SoCs. And these are chips that are on your computer motherboard that basically can control certain things, like the internet connection, and they're their own little environment.

And so Connected Standby allows a computer to go into --

MS. SCANLAN: Objection. Narrative.

THE COURT: Let's ask a question, Counsel. Sustained.

BY MR. CHUN

Q What does a device need for it to have Connected Standby?

A It has to have hardware components, to include solid-state hard drive, system-on-chip hardware, and low-power DRAM, at a minimum.

Q Now, a computer on Connected Standby, will it connect to a wireless network?

A It can connect to previously known wireless networks.

Q Will it connect to a previously unknown network?

A No. It's a security risk to connect to unknown networks.

Q Having looked at the forensics on this laptop, do you have an opinion as to whether this laptop would connect to an unknown network?

A This computer was configured not to connect to any unknown network, only trusted networks. That's the default setting.

Q Showing you what's been marked as Exhibit 18.8, do you recognize that?

A I do. It's a screenshot that I took from the defendant's software registry hive.

Q Fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.8, Your Honor.

MS. SCANLAN: No objection.

THE COURT: 18.8 is admitted.

(Exhibit 18.8 was admitted)

BY MR. CHUN

Q What are we looking at here?

A This is actually the registry entry, or the key, that you could modify if you wanted your computer just to connect to any open wi-fi. And as you see, it's set as "default," which means it will not connect to any open wi-fi. If you wanted to walk around, in a free Starbucks, with no password to connect, you could change this entry, and that way your computer would connect automatically. But by default, these are set not to connect to any untrusted or unknown network.

Q And how is this computer configured?

A As you can see, it's configured as "default." It does not connect to any untrusted, unknown network.

Q Having gone through those exhibits, did you see any forensic artifacts on this computer that indicated a wireless connection after July 5?

A Absolutely not. There are no network connections after July 5 at all.

Q And does that tell you anything about the reliability of evidence on this computer compared to its network activity?

A Well, what it does is, it guarantees that there's no chance that anybody could have remotely logged into this computer, or manipulated the computer, because it had no network connection.

Q Now, how difficult would it be to change a log?

A What kind of log?

Q Let's just say one we saw earlier at 18.1, one of the event logs.

A To change the event log? Well, you could possibly use another program to edit the event log.

Q And do you have an opinion as to whether or not this computer has been tampered with to change all the forensic artifacts relating to remote connections?

A No. There's absolutely no evidence to suggest that this computer was manipulated in any way to change the artifacts, or to do anything like that.

Q And what brings you to that conclusion?

A Well, there are a number of things. As we just walked through, you can see that every artifact is recorded in multiple locations, registry entries, multiple event logs, et cetera. In addition to that, the event logs, although they don't show on the screen, actually are recorded with a sequential number. So every single event log gets a sequential number. And that's how we can determine, if somebody changes the date and time on their computer, the event logs will show out of sequence with the date and time. And so we've checked the sequential numbering, and the integrity of all of the event logs are intact, no tampering has been done.

Q Did you also examine this laptop to see who the last user logged in was?

A I did.

Q And showing you what's been marked as Government Exhibit 18.9, do you recognize that?

A I do. It's a screenshot that I took of an event log off of the defendant's computer.

Q And this is a multipage exhibit. Can you just thumb through there?

A Yes.

Q Is this a fair and accurate copy of the screenshot you took?

A It is.

MR. CHUN: United States moves to admit 18.9, Your Honor.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, I'm sorry, this is a screenshot of what, now?

A This is a screenshot of the event logs from the defendant's computer. This is the security event log, specifically.

Q And the red highlighting is your additions?

A Yes.

MS. SCANLAN: No objection.

THE COURT: 18.9 is admitted.

(Exhibit 18.9 was admitted)

DIRECT EXAMINATION

BY MR. CHUN

Q Mr. Carroll, so what are we looking at here?

A On this page right here, you're looking at the

Event ID 4647, which shows the last time the user account "smaus" logged off of this computer. And this shows that the user logged off on July 5, at 2:24 a.m. And as you can see on the bottom here, it says, "No further user-initiated activity can occur." The user is logged off.

Q Okay. And on the bottom of that page there, it says "Security ID."

What is that?

A The Windows computer doesn't always identify you by your username, in this case "smaus." It identifies you in a number of forensic artifacts by your user security identifier, your SID, which is what you're looking at. There, it ends in 1001.

Q Now, turning to Page 2 of this exhibit, what do we see here?

A This is just further up the list of that same event log. And this is an event log showing a user logon. And here, you see the security identifier of "S-1-5-18." And what that is is the Windows desktop manager. So anything that happens on a Windows computer has to have permissions. And so this is -- the system itself has its own permissions. And so this is the operating system doing something on the computer.

Q And -- sorry. You're looking at the Security ID to see who the user is?

A Yes.

Q And going to Page 3 of this exhibit, what do we see here?

A This is, I believe, the last event log in the security event log, showing, again, a special logon by the operating system.

Q Now, going back to the first page of that exhibit, just magnifying the top portion, I note that there are logons and logoffs, heading upwards in this log, showing days of July 5th and 6th, and onwards to July 11th you saw on Page 3.

Did you check all of those?

A I did.

Q What did you see when you checked all of those?

A As I said, this shows that the user logged off. And after the user logged off, the computer was still powered on, and the system was doing its system maintenance operations. And so these are indications of the system, not a user account, actually conducting those operations.

Q After the red box logoff here, did you see any other person user logons?

A There are no other user logons.

Q So they were all by the system?

A They were all by the system.

Q And what does that tell you about the activity on this computer?

A It says that the computer remained powered on after the user logged off, and the system was doing its typical maintenance operations.

Q And showing you what's been marked as Exhibit 18.10, do you recognize that?

A I do. It's a screenshot that I took of the SAM registry hive off of the defendant's computer.

Q Fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.10.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, the information that's inside the red box, did you add that information?

A If you're talking about the very top box, that is my writing, in red. So anything that you see in red is my writing. And that shows where that SAM registry hive was on the defendant's computer. And then there are two other red boxes, which I highlighted to bring the prosecutor's attention to why I was doing this screenshot.

MS. SCANLAN: No objection.

THE COURT: 18.10 is admitted.

(Exhibit 18.10 was admitted)

MR. CHUN: Thank you, Your Honor.

////

////

DIRECT EXAMINATION

BY MR. CHUN

Q Mr. Carroll, what do we see here, in 18.10?

A As I mentioned, this is the SAM registry hive. Every Windows computer has a series of registry hives. They're like databases. And the SAM registry hive has a list of every user account on the system. So this is what is checked when you log on. It looks there for your permissions to log on to that computer, your password. And this is showing the user account "smaus," which is highlighted here, has a unique security identifier of "1001." And that account, smaus, is associated with a Windows Live ID account of romariomail.ru [sic].

Q Could you actually just spell that out?

A R-O-M-A-R-I-O-G-R-O-L.

Q Would that be a "1"?

A Or "1," yes.

Q @mail.ru?

A @mail.ru.

Q And so what would be the connection between smaus and that e-mail address?

A Starting with Windows 8.1, they wanted you to start logging on to your computer with a Windows Live ID. And so you put in your e-mail address to get a Windows Live ID. And what this is is, for the user account smaus, which you see here, this is the e-mail account that's registered with Microsoft for that account name and that computer.

Q And who would have set that connection up?

A Whoever set up the computer, whoever set up this account called "smaus."

Q So the user of smaus would have tied it to the romario --

MS. SCANLAN: Objection. Leading.

THE COURT: It is leading, Counsel. Sustained.

BY MR. CHUN

Q Would the user of smaus -- what connection would they have made between that and the e-mail shown?

MS. SCANLAN: I object. This is beyond the scope.

THE COURT: It's overruled.

THE WITNESS: As I mentioned, Microsoft wants you to have an e-mail account. And so they ask for an e-mail account name when you're setting up your user accounts on Windows 8 and above computer systems. And so the user that set up this "smaus" set up an e-mail account of this e-mail in order to establish an account on this computer. And so that's how Microsoft now ties activity to the smaus user account on that computer. It's a way Microsoft can better track our user preferences.

Q And turning to Page 2, what do we see here?

A This is another screenshot of the software registry hive. This is a different database, also called a software registry hive. And I took a screenshot of this just to show the full user security identifier. You can see there's the 1001 at the end, that the SAM registry hive we just looked at shows. And this is just the full registry hive. And what this registry key also does, it says that this is the home directory of that user, smaus.

Q And now turning your attention to what's been marked as 18.11, do you recognize this? I'll blow this up a bit so we can see it.

A Yes. This is a screenshot that I took of the output of the SRUM, the system resource usage monitor database --

Q Do you recognize this?

A I do. It's a screenshot that I took off the defendant's computer.

Q Is it a fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.11, Your Honor.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 18.11 was admitted)

BY MR. CHUN

Q And for the record, how many pages is this exhibit, Mr. Carroll?

A A lot. It appears here about 175 pages.

Q Is there numbering in the corner, right-hand corner there?

A 176, yes.

MR. CHUN: Permission to publish, Your Honor?

THE COURT: 18.11 has been admitted. You may publish.

MR. CHUN: Thank you, Your Honor.

BY MR. CHUN

Q And what are we seeing here, at the top of this box here?

A The system resource usage monitor -- we call it SRUM -- this database tracks every application that's running and which user is responsible for running that application. And it also accounts for the energy usage, how much CPU power and energy is that particular application using. And that way, you can tell what's draining your battery, or Microsoft can tell what's draining your battery.

And so as we see here, in the highlight of red, the last applications that were run, that were attributed to a user, as opposed to the system, was the Tor, The Onion Router; and Firefox.

Q And you're gauging that based on which column there?

A Well, this -- the fourth column here has the User ID of which user was responsible for running the application. In Column 3 is the Application ID, or the application name, what program was running. And then Column 2 was the time that that application was recorded by the SRUM database.

Q And what user was that user ID associated with, the one ending in 1001?

A As we just saw, that was the smaus user account.

Q And what about the user below that, the S-1-5- --

A Eighteen. That are all system -- this is the operating system running those processes, again, doing system maintenance, et cetera.

Q And going to the very end of this exhibit, did you examine this computer as to when the last user-engaged activity was?

A I did. And what we just saw on the 5th of July was the last application that was run attributable to a user. Everything after July 5 was actually the system running its processes.

Q And you know that, again, here highlighting the last page -- what would that be based on?

A It's based on the user identifier, the user that ran that application.

Q And that was true for all 175 pages in between, as well?

A That's correct.

Q Now, having looked at these exhibits regarding user login, what is your opinion about the last time a user was logged into this computer?

A Well, it's clear, all the evidence shows that the last user that was logged into the computer was smaus, and the last time that user logged off was July 5, and no other user logged on to this computer in any way after July 5.

Q And in regards to the reliability of data on this computer, what does that tell you?

A The integrity of the computer is complete, solid.

Q Now, earlier there was testimony from the defense witness that this computer had approximately 3,000 files of access dates after July 5.

Did you look into this?

A I did.

Q And did you also examine whether or not there were files that were modified after July 5?

A I did.

Q And the testimony there was, there was about 274 files for modification.

What did you find?

A I saw roughly the same number, 273, 274, total files, although many of those were zero files, or directories, so -- but about the same.

Q And did you review each of those files?

A I did. I reviewed every one of them.

Q And what conclusion did you draw, after reviewing each of those files?

A It was clear, through the review, that all of those were system-related files; that the time stamps had been changed as a result of system-related activity, maintenance activity, antivirus running, et cetera.

Q And what about in regards to the 3,000 or so files with last access dates after July 5?

A I reviewed all those, also; had the same conclusion, that all of those files are a result of, typically, your antivirus. Your Windows indexes your computer so when you're doing searches it knows where your files are. And this type of activity can cause the last access time to be updated.

Q Now, are access dates often used by forensic examiners?

A No.

Q Why not?

A Well, all of your forensic training programs will tell you that the last access date has too many variables that affect the last access date to render any real opinion. This is a perfect example, is, when antivirus runs, it's touching all those last access dates. And a last access date doesn't mean that file was even opened. It just means the system, or something, touched that file.

And starting in Windows Vista, Microsoft actually turned off updating of last access dates on all consumer versions. Only the professional Windows, Windows 8 Professional, Windows 10 Professional, only the professional editions have last access dates even turned on. Microsoft just quit updating them.

Q And based on your training and experience, do you have an opinion as to what caused the file access dates of these 3,000 or so files to change after July 5?

A Absolutely. In looking at all the activity on the computer, what programs were running, and temporal analysis, it was clear that all the last access dates that were touched were a result of antivirus and standard system maintenance-type functions, indexing, et cetera.

Q Showing you what's been marked as Government Exhibit 18.12, do you recognize that?

A I do. It's a screenshot that I took of the USN journal, off of the defendant's computer.

Q Fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.12.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, what is the highlighting in orange?

A The highlighting in just orange, or red, also?

Q Let's just talk about orange, first.

A The highlighting in orange were my highlights showing the Windows -- I'm sorry -- the McAfee Antivirus log files being updated.

Q How about the highlighting in red?

A Also the McAfee Antivirus log files updating. As your antivirus is running, it's updating log files so it can remember what it's doing.

Q What's the difference between the red and orange highlighting here?

A Defense forensic experts had suggested that the -- there was foul play because of the last access times. And what this showed is, there were some specific files in the recent directory that had the last access times updated. And in red shows that about 60 seconds before those files had a last access time stamp change, the Microsoft -- or excuse me -- the McAfee Antivirus log was updated in 120 seconds after. So it was consistent with the antivirus program running.

Q I'm sorry. What was the difference between the red and the orange?

A Before and after.

MS. SCANLAN: Thank you.

I have no objection to this exhibit.

THE COURT: 18.12 is admitted.

(Exhibit 18.12 was admitted)

DIRECT EXAMINATION

BY MR. CHUN

Q Mr. Carroll, what are we looking at here?

A So as I said, this is the user -- I'm sorry -- the USN journal log. And this is sort of, like, Microsoft's black box.

It's trying to record files that are touched on the system so applications can keep track of which files may need updating, or antivirus run, et cetera.

And what we're looking at here is, highlighted in red are the Microsoft service -- Microsoft -- I'm sorry -- the McAfee service hosts log file. So all of these are McAfee service hosts log files. As you can see here, they're being updated just prior to the recent directory files access times being updated. And then in orange, you see it being -- the log files being updated again by McAfee.

Q And what does this log, then, tell you about the activity on this computer after July 5?

A Well, it just shows that the antivirus program is running, scanning files.

Q And how does that affect your opinion as to changes in the last access dates?

A Well, it's just proof that that's what was happening, is that this was one of the maintenance operations that were happening by the operating system, not by a user, that caused those last access times to be updated.

Q And now showing you what's been marked as 18.13, do you recognize that?

A I do. It's a screenshot of the output of the SRUM database application resource log, off of the defendant's computer.

Q Fair and accurate copy?

A It is.

MR. CHUN: United States moves to admit 18.13, Your Honor.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 18.13 was admitted)

BY MR. CHUN

Q And what are we -- sorry about that. What are we looking at here?

A So as I said, the SRUM database is tracking all the applications that are running and which user account is responsible for running that application. And this is after the 5th, when the user logged off. And what you can see is just multiple instances where the McAfee Antivirus program is running. And again, it just further corroborates that the antivirus program was running and was responsible for the updates of the last access times of the files.

Q And this would be -- and then what is that -- what's your opinion in regards to this as to activity on this computer after the 5th?

A Again, it just further confirms, another artifact that confirms, there was no user interaction, because you see that this is the system actually running the McAfee Antivirus program, and that further confirms that the antivirus program was running and checking those files.

Q Now, if you could go ahead and turn to Exhibit 13.40. And you might need a new binder for that. And this was previously admitted.

THE COURT: Counsel, let's let the jury take a quick stretch break. I know we've got ten more minutes before the break.

MR. CHUN: Yes, Your Honor.

THE COURT: Please be seated.

BY MR. CHUN

Q Looking at 13.40, could you go ahead and scan this list for -- this is the government's trial exhibits from the computer. Could you go ahead and scan the list for last access dates occurring after July 5? It might be easier in the binder.

A Okay.

Q And do you see any with a date after July 6?

A I see one, it looks like, here.

Q And which exhibit would that be?

A This would be Line Number 13.6, right here.

Q And looking at 13.6A, if you could just go ahead and read what that is there, in the description.

A "Animated 2Pac ad from desktop."

Q And looking at 13.6A, which is the metadata for that, were you asked to examine the computer for this file?

A I was.

Q And for the integrity of this file?

A I was.

Q What did you look for?

A I looked for the existence of that file on the computer.

Q And how did you do that?

A With our forensic software, FTK, I examined, looking exactly for that file.

Q And what did you do next?

A Well, I found the -- that particular file in the current operating system. But Windows has this feature called Volume Shadow Copies. And what that is is, Windows takes a snapshot of your computer, every once in a while. And typical Windows computers will have at least three or four snapshots of your computer. So if something bad happens, you can roll back to a previous date. And these are called Volume Shadow Copies.

And what I did is, I looked --

Q I'm sorry. Let me stop you.

A shadow -- or Volume Shadow Copy?

A Uh-huh.

Q So what, specifically, is a Volume Shadow Copy?

A A Volume Shadow Copy is that snapshot in time of files on your computer system.

Q And so that would be from when?

A Well, there were, I believe, four different snapshots, or four different Volume Shadow Copies on the defendant's computer.

Q And how does that relate to your search of integrity for this file?

A Well, the nice thing about Volume Shadow Copies is, they are a snapshot of the file. And so one of the things that I will do, particularly in cases like this where someone misinterprets a last access date being updated, you can go back to a Volume Shadow Copy. You can find that exact file, in the Volume Shadow Copies, prior to that last access date being updated. You can actually check that file. There's a cryptographic hash value that you can get. It's a digital fingerprint for every file. And you can check to see if that file -- exactly the same -- and you can see that it was exactly the same as the one that had the date/time stamp after July 5.

Q And were you able to find that one banner?

A Yes.

Q And how did you compare that they were the same?

A Again, there's -- not to get too technical, but there's this mathematical algorithm that you can run against any file or data stream. And it gives you a digital fingerprint, a long alphanumeric value, that says, "This is the digital fingerprint of this file." If anything in that file is changed, even so much as an extra space or a period on that file, that value, that digital fingerprint, will be radically different.

And so I did a hash -- that's what they're called. The digital fingerprints are called a "hash." I did a hash of the banner on the current operating system. And then I found that, also, in Volume Shadow Copies, those previous snapshots in time, did a hash of that file in the Volume Shadows Copies, and they were identical. They were exactly the same.

Q And were those Volume Shadow Copies from before July 5?

A They were.

Q And was that the only trial exhibit, on that list you saw from defendant's laptop, that had a date of July 6 or after? And you can go back to -- if you like, it was 13.40.

A I looked at a number of files. I did a random sampling of a number of files that had last access dates after July 5, found all those files in Volume Shadow Copies --

MS. SCANLAN: Objection. This is nonresponsive.

THE COURT: It's overruled on those grounds, Counsel.

THE WITNESS: Found all of those files in Volume Shadow Copies, and all were exactly the same, which just proves definitively, because of the digital fingerprint, nothing was changed in those files.

BY MR. CHUN

Q Showing you what's been marked as 18.17, what are we looking at here?

A This is a snapshot --

Q I'm sorry. Do you recognize it?

A I do.

Q Fair and accurate copy of a snapshot you took?

A It is.

MR. CHUN: United States moves to admit Exhibit 18.17.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 18.17 was admitted)

BY MR. CHUN

Q And this is very hard to see, because the text is small, so let's go column by column.

What are we looking at here, Mr. Carroll?

A Okay. This first column is the name of the files. This is just a small number of the name of files that I looked at. And you can see that the first entry, e-dump24.txt.lnk, was in the current directory. So this is the active directory of the computer. And then I found that exact same file in a Volume Shadow Copy. This is a snapshot. And I did this on every one of these files. You see these files in the current. The first listing will be the current location, the active computer. And the second entry is that same file in a Volume Shadow Copy.

Q Now, moving to the next columns over -- I'll do the next three -- what do we see in these columns?

A Remember I told you that a hash value is a digital fingerprint? So this first column has a heading of "SHA1."

That is the digital fingerprint for that -- each of those files. And you can see the digital fingerprint in each is exactly the same. So the one that was on the current computer, digital fingerprint was this. And then the Volume Shadow Copy, the digital fingerprint was this. And then these next two columns that you see here are the created and accessed date.

Q So for that first one, it shows an access date of July 13; is that correct?

A That was the -- that was correct. That's on the active hard drive, the computer.

Q And then what's that date below it?

A The below is the last access date of that same exact file on that snapshot, that Volume Shadow Copy.

Q And the matching SHA1 columns, then, tell you what about those two files?

A That those two files are an exact duplicate of each other, no modifications, no changes whatsoever occurred to the contents of those files.

Q And just to show, what would be the last column of that exhibit?

A The last column, every file has a creation, modified, and access date. And this is just the modified date column.

THE COURT: Counsel, it's 2:45. Is this a convenient time to take a recess?

MR. CHUN: Yes, Your Honor.

THE COURT: Members of the jury, we'll take our afternoon break.

(Jury exits the courtroom)

THE COURT: Counsel for the government, anything to take up?

MR. CHUN: No, Your Honor.

THE COURT: Defense, anything to take up?

MS. SCANLAN: No, Your Honor.

THE COURT: We'll be at recess.

(Recess)

(Jury enters the courtroom)

THE COURT: Counsel, you may continue your direct examination of the witness.

MR. CHUN: Thank you, Your Honor.

BY MR. CHUN

Q We were just talking about Shadow Volume Copies [sic].

How easy would it be to plant a file inside a Shadow Volume Copy?

A No.

Q What do you mean?

A No, it would not be easy.

Q How difficult would it be?

A It would be very difficult. I don't know of a way to plant a file on a Volume Shadow Copy.

Q And earlier we had heard testimony that it would be easy to remotely log in and push files onto the defendant's laptop and then hide its tracks, by editing logs and such.

Do you agree with that opinion?

A No, not at all.

Q Why not?

A Well, as we just saw, for every action that's on a Windows computer there are multiple forensic artifacts that are created. To start off with, the computer would have to be connected to a network. And it's clear, there's no doubt, that this computer was never connected to a network after July 5. So that's the first thing. So that eliminates anybody logging on.

But then even if somebody tried to plant something on his computer, again, there would be multiple forensic artifacts to show that that actually happened.

Q And is your examination looking for those things?

A Yes. Our examination is looking for any anomalies, whether the integrity of the computer is pristine, is there anything to suggest that the evidence shouldn't be trusted. And no evidence was on the computer to suggest that.

Q And earlier there was also testimony that 3,000 changes of an access date was so much volume it could only indicate somebody up to nefarious activities, or some issue.

Do you agree?

A No, not at all.

Q What is your opinion about 3,000 or so last access dates changing?

A Well, if we start with the premise that no forensic examiner really attributes anything to the last access time, because, as we're all trained, there are far too many variables that affect the last access time to render an opinion, the evidence on the computer clearly shows that the last access time changed were a result of typical system maintenance processes, antivirus, there was a spy hunter, all these programs are running. We saw through numerous forensic artifacts that every application and every process that was running after July 5 was not the result of a user. It was the result of the system; again, just further evidence that this is maintenance. This is standard system maintenance. So, no, that's just not possible.

Q Does 3,000 seem like a number that's too large for file access dates changing when a system is in Connected Standby?

A No. It's relatively consistent.

Q And having examined this computer as a whole, what is your opinion about its reliability?

A There's no evidence on this computer anywhere to suggest that the reliability is in question. The computer is intact. The integrity of the files are intact. Not only that, but I did verification of numerous files in Volume Shadow Copies, just on the chance that some file may have been planted, looking at the hash value, that digital fingerprint, all the same in each Volume Shadow Copy. There's just no evidence to suggest or even support that suggestion, by any competent forensic examiner.

MR. CHUN: No further questions, Your Honor.

THE COURT: Cross examination?

CROSS EXAMINATION

BY MS. SCANLAN

Q Mr. Carroll, you work for the Department of Justice; correct?

A Yes, ma'am.

Q And the -- one of the divisions of the Department of Justice is the U.S. Attorney's Office?

A Yes, ma'am.

Q And the U.S. Attorney's Office would be the prosecuting agency in this case; correct?

A Correct.

Q Are you ever hired as an expert by criminal defense attorneys?

A I've been asked, but I can't take outside employment without authorization from the Department of Justice; so, no. I conduct training with defense attorneys, but not hired as an expert.

Q Okay. You run a lab; right?

A I do.

Q Do you have an evidence vault?

A I do.

Q And do you put the evidence in the vault when you're not examining it?

A Well, the nice thing about our lab is, we don't typically receive actual evidence. We only receive copies.

Q So what goes in your vault, then?

A On those rare occasions where perhaps an investigative agency can't image a hard drive, they have a special piece of equipment, if they send that to us, that will go in when we're not with it.

Q And what are the protocols for access to your vault?

A There's multi-factor authentication, so you have to swipe in -- first of all, you have to get into our building, get past the guards, swipe into our floor, then swipe into our office, then swipe into the evidence room, PIN codes to make sure that nobody has your card. So there's a number of hoops that you have to jump through.

Q Is there a vault log?

A Yes.

Q What's a vault log?

MR. CHUN: Objection, Your Honor. Scope.

THE COURT: It's overruled. I'll permit some latitude.

THE WITNESS: A vault log?

BY MS. SCANLAN

Q Yes.

A It's just a log of who enters and exits.

Q Do you have one of those for your vault?

A Ours is automated, because it's all electronic; so, yes.

Q So does it record everyone who enters and exits the vault log?

A It records who enters. We don't swipe out of the log.

Q You just swipe in?

A Yes, ma'am.

Q And you're aware that there were people who entered and exited the vault log where this laptop was kept, in this case, without writing it down in a vault log; correct?

A I've heard some discussion about it, but I'm not exactly sure about that.

Q These event logs; right?

A Yes.

Q Okay. So just a basic yes-or-no question, can they be altered?

A A yes or no, I have to go with yes.

Q Okay. And the McAfee Antivirus program that was running on the laptop, you're familiar with that?

A I am.

Q That can run when a user is using the computer; correct?

A Correct.

MS. SCANLAN: I have nothing further.

THE COURT: Any redirect?

MR. CHUN: No, Your Honor.

THE COURT: Any objection to this witness being excused, by the government?

MR. CHUN: One moment, Your Honor. Could we have one moment, Your Honor?

THE COURT: You may.

MR. CHUN: No objection, Your Honor.

THE COURT: All right. Any objection by the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you, sir. You're excused. You may step down.

Counsel for the government, any additional rebuttal evidence or testimony?

MR. CHUN: No, Your Honor.

THE COURT: Anything further from the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: All right. Ladies and gentlemen of the jury, your work today has come to an end. And as I mentioned yesterday, we need to have a conference regarding jury instructions so that when you come in tomorrow morning at 9:00, you'll receive a copy of the jury instructions. And I'll be reading the jury instructions to you, and then we'll begin with the closing remarks after that.

So we need to have you go and enjoy the balance of the day, and we'll see you all tomorrow morning, ready to go at 9:00 a.m. Have a good evening.

(Jury exits the courtroom)

THE COURT: Did each of the parties receive their copy of the Court's proposed jury instructions?

MR. WILKINSON: We have, Your Honor.

MS. SCANLAN: Yes, Your Honor.

THE COURT: All right. Counsel, we're going to go over those at this time. My law clerk went to go get my copy. I mistakenly left it, after the break.

But, nonetheless, there's only two questions that I have for the parties. Are there any exceptions with respect to the instructions as proposed by the Court? Are there any exceptions with respect to the Court's failure to give any proposed instructions; same question for both sides.

So with that, counsel for the government, any exceptions with respect to the instructions as proposed by the Court?

MR. WILKINSON: Yes, Your Honor.

THE COURT: All right. Let me hear them.

MR. WILKINSON: Your Honor, the first issue pertains to proposed Instruction Number 10.

THE COURT: Let me catch up with you.

MR. WILKINSON: This is the pattern instruction for 404(b) evidence. The government has not offered 404(b) evidence during this case. The defense took the position in a pretrial pleading that some of the evidence was 404(b) evidence. The Court denied that motion, at Docket 396, and specifically found that the evidence was not other -- evidence of other acts implicating 404(b). So we believe that instruction is not necessary.

THE COURT: Okay.

MR. WILKINSON: Next one is Instruction 21.

THE COURT: Let me catch up with you.

MR. WILKINSON: And for this, we would propose the addition of some prefatory language, which is as follows --

THE COURT: And do you have a draft copy that you could give the Court, Counsel?

MR. WILKINSON: I can write one out. It's not too long. But I could write one out.

THE COURT: Let me hear what your proposed changes are.

MR. WILKINSON: "If you find the defendant guilty of any count of wire fraud, you will then be asked to determine if that act of wire fraud affected a financial institution."

THE COURT: Just a second. Okay.

MR. WILKINSON: The reason for that is that we're defining "financial institution" in that instruction. But since that doesn't relate to any element that's otherwise explained, I think the jury will be left to wonder why we're defining financial institution. So this just gives them some context of why they need to know what it means.

THE COURT: I think, from the defense perspective -- I'm not trying to take their thunder away on that issue -- but the concern the Court has with your proposal is, that's language that's typically found in a verdict form, as opposed to being included in the body of the jury instructions. I don't want to have suggestions as to what the jury has already done in the content of the jury instructions, because that appears to suggest that the Court has an opinion. It may be a vague reference to a finding. But nonetheless, it says, "If you find the defendant guilty..." That type of language shouldn't be in a jury instruction preceding an instruction. It's more appropriate in a verdict form. But your exception is noted.

Next one?

MR. WILKINSON: Thank you, Your Honor.

The next one is Item 26, Instruction 26.

THE COURT: Let me catch up with you. Okay. I'm with you.

MR. WILKINSON: And the Court had put a note on this instruction that it needs to be reconciled with the verdict form.

THE COURT: Correct.

MR. WILKINSON: So the issue here is that the indictment -- this is the possession count -- the indictment described a range of time when the defendant possessed 15 or more access devices. The instruction, however, says that -- it requires the jury to find that the defendant possessed the access devices at the same time. And it was our thought that it would be confusing to the jury to provide a range of time, and then tell them that they have to find this happened at a certain point in time.

And so our proposal was just to take out -- change it from a range into a specific date, and take out the end date, and so just have the begin date be the date that is charged, or that they need to find. And that's consistent with the -- that was the instruction we proposed and also the -- what we had proposed for the verdict form.

THE COURT: Okay. Next one?

MR. WILKINSON: The next item is Number 27.

THE COURT: Okay.

MR. WILKINSON: This is the definition of access device. We would propose the addition of a sentence at the end that says, "A credit card is an access device." This is clearly an accurate statement of the law. And we'd direct the Court to *U.S. vs. Onyesoh*, O-N-Y-E-S-A-H, [sic], at 674 F.3d, 1157, Page 1159. It's a Ninth Circuit opinion from 2012.

And the statutory definition is there, but we think that this leaves the jury to interpret the law. And where the Court can provide direct guidance on what the law is, we think it's appropriate that it do so, and that the jury not be left to interpret the statute.

THE COURT: Counsel, if you look on Line 3, that reads, "An access device means any card."

Would that not necessarily include credit card? Or does that appear to be redundant, if the Court adds the language that you're suggesting?

MR. WILKINSON: I mean, it doesn't specifically say a "credit card." "Credit card" is the term we've been using. It also doesn't specify the card number, I don't believe.

So it just says "any card," and we've been talking about card numbers. We think it's clearer guidance. And it's clearly accurate, so I don't think there's any reason not to do it.

THE COURT: Okay.

MR. WILKINSON: And then the last issue is on Instruction 29 --

THE COURT: Let me catch up with you. All right.

MR. WILKINSON: -- Line 12. It currently states, "An access device is a means of identification." And just for clarity, we would propose inserting a clause that would say, "An access device," and then the insertion is, "as defined in Instruction 27," "is a means of identification," just so that the jury knows where to look if they want to understand what an access device is.

THE COURT: Okay.

MR. WILKINSON: And that's all we have.

THE COURT: Okay. So that covers both categories of questions the Court proposed as far as exceptions?

MR. WILKINSON: It does, Your Honor.

THE COURT: Thank you, Counsel.

And, Counsel, as far as the verdict form, you'll note that the Court had two forms of the verdict form.

Any objection to the verdict form as proposed by the Court?

MR. WILKINSON: No, Your Honor.

THE COURT: All right. Thank you.

Counsel for the defense, your exceptions? Again, two different categories.

MS. SCANLAN: And, Your Honor, did the Court wish to hear from the defense regarding the government objections?

THE COURT: Yes, certainly.

MS. SCANLAN: As to -- and I think this is the only one I didn't write down the number for -- is it 10, which is the 404(b) instruction?

THE COURT: That's correct.

MS. SCANLAN: The jury heard and saw evidence of multiple other acts that could be considered bad acts, or other crimes. For instance, there was all the pictures of the money, that were introduced by the government. There were people testifying from other businesses.

Now, I know that there was a whole discussion pretrial about whether those are other acts. But it's still the defense position, especially in light of the testimony through trial, that there hasn't been a sufficient connection between those other businesses and the charged counts for it to be anything other than other acts evidence in this particular case. So we would agree with the insertion of that instruction.

Instruction 21, I think the Court essentially said what the defense objection is to this. It's the same objection that we had for the government's instructions in regards to the language the government wants to add about finding somebody guilty, and putting it in the middle of this instruction. So the defense objection, at that time, stands, which is that it goes in the verdict form.

THE COURT: Okay.

MS. SCANLAN: Instruction 26 with the date ranges -- well, actually, backing up, Instruction 26, in general, I would object to the insertion of the language "access device fraud," at the end of Line 3, beginning of Line 4. So the actual -- the offense is the unlawful possession of 15 or more access devices.

THE COURT: Wait a second, Counsel. Which one?

MS. SCANLAN: I apologize, Your Honor. It's the end of Line 3, beginning of Line 4.

THE COURT: Okay.

MS. SCANLAN: This insertion of "access device fraud" was done by the government, in their proposed instruction, and it's not a part of the -- that's not part of the definition of the offense. The offense is the unlawful possession of 15 or more access devices. So I think having it categorized in the instruction as "access device fraud" is essentially a comment on what the nature of the offense is.

And then we have the date ranges. As far as I understand it, they charged this as the possession being over this period of time. And so it seems a little unfair now to come back and say, "No, it's not this period of time. We're electing this one day." It's not "on or between." It's, "These are the dates when the possession occurred." I'm not sure we get to change that now. For one thing, they're inconsistent, obviously. But to change it now is prejudicial to the defense.

THE COURT: And how so, Counsel?

MS. SCANLAN: Well, the way that it's been charged, the government needs to prove the possession, as I believe Mr. Wilkinson just said, during this time period, so over -- this continuous possession over these date ranges. That's how they've charged it. That's how they've presented it. And so to go back now and elect one of those dates for each count, at the end of the trial, changes the nature of what needs to be proved.

THE COURT: Okay.

MS. SCANLAN: Instruction 29.

THE COURT: Just one second. Let me catch up with you. Okay.

MS. SCANLAN: This -- for one, the -- Line 11 has the term "access device fraud" again. I think it would be much clearer if this stated the actual title of the offense, rather than this new title.

THE COURT: Which should be, according to the defense?

MS. SCANLAN: Possession of 15 or more unauthorized access devices.

THE COURT: Okay.

MS. SCANLAN: The government suggested that the access device definition should refer back to the other instruction. I would suggest that the access device definition does not need to be in this instruction. It's defined elsewhere. So we don't need to define it and then re-refer the jury to another definition.

THE COURT: Okay.

MS. SCANLAN: As for -- so that was the government's issues.

As for the defense exceptions, Instruction Number 6 --

THE COURT: Let me go back, Counsel.

MS. SCANLAN: The defense has proposed the insertion of language from the comment to the Ninth Circuit Model Jury Instruction 1.5.

THE COURT: So it's Instruction Number 6, again?

MS. SCANLAN: Yes. So 1.5 and 3.8, both being the direct and circumstantial evidence instruction.

THE COURT: Yes.

MS. SCANLAN: The language that was suggested by the defense is on Page 3 of Docket 378. The comments suggest that this language may be appropriate to give an example of the difference between circumstantial and direct evidence. It's a paragraph. But it's essentially the whole thing about the sidewalk being wet and the rain.

THE COURT: Let me ask you a question, Counsel.

You and Mr. Browne are very well-versed and experienced in criminal practice; correct?

MS. SCANLAN: Uh-oh. Okay.

THE COURT: All right. "Okay" doesn't answer the question.

Yes?

MS. SCANLAN: Yes.

THE COURT: Now, have you seen any other court, other than the ones cited, where it's not mandatory, but it's optional language, or another court that you've tried a case in, has given the alternative instruction with an example of what circumstantial evidence would be? Usually that's reserved for the lawyers, to give examples. And I could give you a laundry list of examples of what lawyers have given me about what's circumstantial evidence, from the rain, the snow, and they go on and on. You've probably used some of these. I know Mr. Browne has.

So have you ever seen another case, Counsel, where that alternate language has been used?

MS. SCANLAN: My answer, Your Honor, is, I have never suggested it before, so I don't know what those other courts would have done with it.

THE COURT: Have you ever seen or heard of another court giving that alternative language that you suggested, proposed to the Court, in the instructions; yes or no?

MS. SCANLAN: No.

THE COURT: Okay. Let's move forward.

MS. SCANLAN: All right.

THE COURT: Next exception, Counsel?

MS. SCANLAN: Instruction Number 15.

THE COURT: Okay. All right.

MS. SCANLAN: So this is the instruction regarding the use of an undercover agent.

THE COURT: Okay.

MS. SCANLAN: The comments that are below the instruction are correct, that the defense objected to this instruction. And I would stand by that, because this did not become an issue in this case. So this instruction is appropriate when the defense essentially tries to insinuate, through cross examination or testimony, that the agent should not behave in this way. But that's not what happened here.

So at this point now, we're just essentially telling the jury that it's okay that they did this, even though no one has disputed that fact. And that is why the comments suggest there are specific areas when this instruction is appropriate. And this would not be one of those; so entrapment, when entrapment is an issue, or when it's raised that there's improper undercover conduct.

THE COURT: And just so we're on the same page, Counsel, the reason the Court was considering including it is because there was some communication earlier, and testimony by witnesses, where they were serving, so to speak, in an undercover capacity, attempting to purchase -- or did, in fact, purchase -- credit cards using government funds. So we're on the same page, that that was the evidence before the Court.

MS. SCANLAN: Yes, Your Honor. We're on the same page that that was the evidence. What I'm saying is that this instruction, from our perspective, is only appropriate when that evidence is in some way questioned in an entrapment scenario, or when the defense suggests that what they did as undercover agents is inappropriate.

THE COURT: Okay. I got you. Let's go to the next one.

MS. SCANLAN: Number 18.

THE COURT: Okay.

MS. SCANLAN: The government has added language to the model instruction here. And that language is repeated in Instruction 18. So it starts on Line 22, at the very end of that line, and then goes to the end of Line 25.

THE COURT: "It does not matter whether," that line?

MS. SCANLAN: Yes. This is additional information the government has suggested be added to this instruction. And I don't think this is a necessary or appropriate addition to the model instruction.

And then, of course, in terms of Instruction 18, 24, 25, and 26, the defense objects to the use of these charts.

THE COURT: And you don't dispute that those are a part of the indictment; correct, Counsel?

MS. SCANLAN: Correct.

THE COURT: Okay.

MS. SCANLAN: So the dispute is that this invites the jury to decide all of these counts as one issue. So instead of separating them out and really showing, essentially in a paper form, that these are all separate offenses they have to decide on, when you have a chart with all the counts, and each of the allegations for the counts like this -- you know, the idea is, you go in, and you make a decision about all of these, and then you flip to the next one. That's the objection.

THE COURT: Well, let me ask you this, Counsel. The Court has given Instruction -- and I'll give you the exact number -- Number 8, which is, "A separate crime is charged against the defendant in each count. You must decide each count separately. The verdict on one count should not control your verdict on any other count." And the next is Number 9, "You're here only to determine whether the defendant is guilty or not guilty of the charges in the indictment. And the defendant's not on trial for any other conduct or offense not charged in the indictment."

So doesn't that address any concern you have, Counsel, that the jury would possibly blend all these charges together, and not make separate determinations?

MS. SCANLAN: It doesn't, Your Honor. I think, obviously, that instruction is helpful on that front. But the melding of the counts, as opposed to having them individually laid out, is essentially another comment on the grouping of the evidence and the counts.

THE COURT: So you suggest that the Court should have a separate instruction for each one of these counts?

MS. SCANLAN: Correct.

THE COURT: Counsel, have you seen, in the case of *United States vs. Jinian*, J-I-N-I-A-N -- and the reason I cited that case, Counsel, for the benefit of the parties, is because, as I read through that case, there did not appear to be any concern expressed by the Court when there was a consolidation of the charges. I think that particular paragraph in that case even talks about the same format that the government used.

Are you aware of any other cases where there's a prohibition on consolidation in the fashion as proposed by the government?

MS. SCANLAN: No. But I would note that my understanding, in that case, is that the defense didn't raise that as an objection.

THE COURT: I understand that. But I'm indicating that there was no concern expressed by the Ninth Circuit by the fact that that was done in that format, whether raised by the defense or not.

MS. SCANLAN: Okay.

THE COURT: All right. Let's go to the next one, Counsel.

MS. SCANLAN: Instruction 30, Your Honor.

THE COURT: Okay. Let me catch up with you.

Okay. I'm with you.

MS. SCANLAN: So this instruction is for aiding and abetting. I don't think there has been a threshold showing of Mr. Seleznev aiding or abetting the acts of anyone else.

So some of the witnesses, some of the agents, have testified that they believed there were other people involved. So they believed that support was not the same person as the administrator, on one of the websites, for example. Or they believed that, although they think Mr. Seleznev is, I think it was, bulba, the other people who did stuff -- or track2 -- after his arrest, those are other people who are involved in the same thing.

But to aid and abet, we need evidence that Mr. Seleznev actually aided, counseled, commanded, induced, or procured someone to do something. And there really hasn't been any testimony about the relationship, or any alleged relationship, between Mr. Seleznev and these mysterious, I think as Detective Dunn called them, "co-conspirators." So it's not just enough to say that there might have been more people. There has to be some actual threshold showing that he was doing things that would constitute aiding and abetting.

The other separate issue, if the Court chooses to give this instruction, is, Line 27 refers to, "The government is not required to prove precisely which defendant actually committed the crime." And in the context of this case, I mean, obviously, this instruction is normally used in cases with co-defendants. But we don't have co-defendants, so I think this is going to be very confusing.

THE COURT: Okay.

MS. SCANLAN: We take no other exceptions to the jury instructions. We did take exception to the verdict forms.

THE COURT: Okay. Let me hear the exceptions to the verdict form.

MS. SCANLAN: The defense has suggested, as the Court is aware, a different format of verdict form for this, where the counts are not all consolidated onto verdict forms that are, again, grouped by type of offense. So -- and specifically, that the -- essentially the special verdict findings, so regarding the financial institution, for instance, on Counts 1 through 11, that those special verdicts should be separate verdict forms from the verdict on the substantive count.

I think we also suggested -- we did -- a different form of language regarding -- yes -- regarding the special verdict inquiries. So it's Docket 378, Page 14.

THE COURT: Page 14?

MS. SCANLAN: Yes, Your Honor.

THE COURT: That's the last page; right? Okay.

MS. SCANLAN: I apologize. Page 14 of the exhibits, so 378.1.

THE COURT: Oh, I'm sorry.

So what's your question, Counsel? What's your point?

MS. SCANLAN: This -- 378.1 is the language that was suggested by the defense for the special verdict forms --

THE COURT: Okay.

MS. SCANLAN: -- which starts with, you know, if you find the defendant not guilty of this particular offense, of Count 1, then you leave the special verdict form blank. So it starts with that idea. And then if you found the person guilty, then you go on to make a decision about the second question.

THE COURT: Okay.

MS. SCANLAN: I also think it's somewhat unusual to have the guilty -- have the guilty on the left and the not guilty on the right. I don't have an example of that. I would just say that I've never seen it formatted that way. Usually, the not guilty would be the first choice, and the guilty is the second.

THE COURT: I agree with that, Counsel. I think that's traditionally what this Court's done. So we'll make that change without having any question about it.

MS. SCANLAN: And then I know there's a lot of counts. But we are, again, just making an exception to the format of the verdict forms in terms of the grouping of the counts, but also the grouping of the substantive verdicts with the special verdicts. And that's it.

THE COURT: Okay. All right. Thank you, Counsel.

Counsel for the government, do you wish to respond to any of the things noted by counsel for the defense?

MR. WILKINSON: Yes, Your Honor.

On the 404(b) evidence, Instruction 10, defendant raises two issues that they believe are 404(b). One is just the pictures of money. Pictures of money is not an act. It's just pictures of money. So I don't think that there's any theory under which that would qualify as 404(b).

And then the second item was the other businesses that were not charged in the indictment -- or listed as specific counts. And that was the exact topic of the Court's order that I referenced earlier. So that clearly does not qualify.

THE COURT: Okay.

MR. WILKINSON: Instruction 26, which is the issue about the possession charge, the defense indicates that it would somehow make our job easier, or kind of lower our burden, to limit it to a single date. And I think that the opposite is true. As -- if we were to treat it as a period of time, the way the instruction reads, as long as the defendant possessed those credit cards at some point in time within that period, whether it be two weeks or two months, the jury would be able to find the defendant guilty. We are confining ourselves to a reasonable period, to, you know, the date that's noted in there, and then, as the instructions say, a reasonable time around that. So it makes our obligation harder. We're, nonetheless, you know, proposing it, just for clarity's sake.

There's no issue of unfairness here, because the indictment provided notice, as it's required to do, to the defendant, of the period of time we were talking about. And we are just narrowing our focus, rather than broadening it.

THE COURT: Do you see any issue, Counsel, between -- any inconsistency between what was charged in the indictment, which is an on-or-about date, or a range of dates, and the specifics of what the government's now proving? Because the defense says, well, now there's prejudice, because we were preparing one defense one way, and now the government spring-loads on us and says, we're only going on one particular date.

MR. WILKINSON: I think if we'd gone the opposite way, if we'd said we have to prove that you did it on December 10, and now we were trying to expand the period of time, there would be a risk of prejudice. Since we're narrowing the focus, we're charging something that was a date that was charged, we're just not trying -- we're just basically stripping back dates that were also charged. So I don't see how there could be any prejudice there. If anything, it would be helpful to the defense.

THE COURT: Okay.

MR. WILKINSON: On Instruction 29, the issue about the title and the use of "access device fraud," we're fine with that change. We don't see a problem with that. So we would agree with changing that to "possession of access devices," rather than "access device fraud."

THE COURT: Okay.

MR. WILKINSON: Then on the defendant's exceptions, a few that we'd like to respond to. On Number 15, regarding --

THE COURT: Just one second. Okay.

MR. WILKINSON: -- regarding the use of undercover agents, it's clearly an issue in this case. We've had, I think, at least three witnesses testify that they participated as undercover agents. There was some questioning that -- about -- where counsel asked the agent, "Were you using a fake name" or a false name, something along those lines, "when you were doing this?" We kind of -- we took that to mean that that might be implying that the agent was doing something improper.

I'd say, at a minimum, if the Court's not going to get -- give the instruction, we'd ask that there be a commitment from the defense that they're not going to argue in closing that the agents somehow behaved improperly by using undercover names.

MS. SCANLAN: I will make that commitment, Your Honor. We're not going to make that argument.

THE COURT: All right. Then, based on that concession, Counsel, do you need to include or keep the Instruction Number 15?

MR. WILKINSON: No. That's fine to remove that.

THE COURT: Based upon a stipulation from the defense, the Court will strike from the instructions Instruction Number 15.

MR. WILKINSON: On Instruction 18, the wire fraud instruction, there, I think, are two exceptions there. One is some additional language that we had proposed about the scheme needing to be successful, and the wires not needing to contain false statements. I don't think defense is disagreeing that that's an accurate statement of the law. And the law in support of that is cited at Page 14 of our trial brief. It's the Supreme Court's *Neder* decision, N-E-D-E-R.

With respect to the second exception there, which is to the charts, we offer -- we use these charts now really as a matter of routine, just for clarity, where there are multiple counts like this. And I think that's reflected in the fact, as I understand it, the jury had asked the Court whether they'll be provided with a chart. And I think that just reflects the need, when you have 40 counts, to try and categorize things these ways. So I think there's an important benefit of doing it this way.

THE COURT: Just to make sure, that communication was shared with both sides.

MS. SCANLAN: Yes, Your Honor.

THE COURT: Okay.

MR. WILKINSON: The second point -- so I guess the objection here, though, is that the charts somehow cause the jury to consider everything all together, and doesn't -- not view the counts separately. The Court's already noted that there's an instruction that expressly directs them to consider each count separately.

In addition to that, the verdict form separates out each count, so they have to mark each one separately. So I don't think that leaves any questions about that. And on top of that, I think the fact that the chart has discreet items actually makes visually clear that each one of these is a specific item. We have Count 1. We have Count 2. We have Count 3. We have Count 4. So the notion that somehow this conflates all the counts, I think doesn't make a lot of sense.

THE COURT: Okay.

MR. WILKINSON: With respect to aiding and abetting, which is Instruction 30, we do believe that instruction is appropriate here. There's been extensive testimony that there were others in the organization, that the defendant has people who support him and help him out. So the question is whether a reasonable jury could find that, with some of these acts, you know, one of the wires, perhaps, could it have been one of his support people who actually did the wire, caused the wire to happen, as part of the defendant's enterprise. And I think the jury could reasonably conclude that and could, therefore, find an aiding and abetting instruction is appropriate.

THE COURT: Okay.

MR. WILKINSON: Lastly, on the verdict form, the defendant has objected to the use of -- or wants to separate out the counts from the special verdict forms, or the special verdict questions.

We have 40 counts here. Many of these counts ask separate questions. I think it's important, to help this jury, that we try to make this as clear as possible. And separating everything out so that they have to go through a decision-making process once, and then go back and revisit each count, 40 counts, I think is going to be really onerous for the jury. And so we propose that we group things together by count. I think it makes sense that way, and I can't see what the prejudice would be of grouping them together.

And then I guess the last issue was the addition of additional language about, if you find the defendant not guilty, then you should leave this entry blank; and then if you find the defendant guilty, then you should answer the question about the financial institution, or whatever it is. That seems fair and appropriate, and we wouldn't object to that.

THE COURT: I'll make that affirmative determination now, that that will be included.

MR. WILKINSON: No further responses.

THE COURT: All right. Counsel, then, you can see the instructions that will be coming out to the parties as the Court's final determination. I've made some preliminary rulings on some of the jury instructions so that you know exactly where the Court stands. I'll go back in and take under advisement the arguments that you've made. I'll go back and look and see if there's any particular cases. Government counsel -- I think it was the *Neder* decision that the government pointed out. And there's also one that was pointed out, the *Onyesoh*, 674 F.3d 1157. So if there's any other cases that were cited by the parties or cross-referenced in the trial briefs, the Court will go back and revisit those. Nonetheless, counsel, you'll receive the jury instructions from the Court in the next couple hours so that you'll know exactly what the instructions are this evening.

We'll begin tomorrow morning, without any other interruptions, and begin tomorrow morning with me reading the instructions to the jury. Each member of the jury will receive their own copy of the jury instructions, with some preliminary statements about theirs to keep or mark and do whatever they'd like to do, and then we'll go right into closing arguments.

Now, the thing that would be helpful for the Court, you're not bound to this, but it's helpful for scheduling, is, I need to know who will be giving closing remarks and approximate times.

Counsel for the government, who will be giving closing remarks?

MR. BARBOSA: Your Honor, I'll be giving closing remarks. And I believe approximately 45 minutes to one hour.

MR. BROWNE: Excuse me. Is rebuttal going to be by someone else?

THE COURT: Just a second, Counsel. Mr. Browne, we haven't gotten that far.

So counsel for the defense, who will be giving closing remarks?

MS. SCANLAN: I will, Your Honor. I would say about 45 minutes.

THE COURT: And then, counsel for the government, who will be giving rebuttal?

MR. CHUN: That would be me, Your Honor. And 15 minutes, Your Honor.

THE COURT: Again, Counsel, you're not tied to this, by any means. It just helps me for scheduling.

And I'll also let you know, I'll try and give you a pretty wide range of opportunity to complete your remarks before the jury without having to break for breaks and recesses. I hope that we can get through closing arguments by the government and the Court reading the instructions -- because I always budget a half an hour for me, and if you're going to stay within 45 minutes to an hour, we should be close to the 10:30 time period and take our break around that time.

If it looks like you're starting to go much past the break time, I may ask, "Counsel, how much more time do you need to complete your closing remarks?" I'll apologize in advance if that breaks your flow of thought. But you should know your case well enough so that a brief interruption shouldn't destroy your opportunity to continue.

Counsel for the defense, same thing would apply. I would suspect that we'd be able to get your closing remarks in from the afternoon -- from the morning break, and certainly before lunch. And we may go into the lunch hour if counsel for the government represents that rebuttal is only going to be 15 minutes.

So I suspect, Counsel, we'll be able to get everything done tomorrow morning on a good note, to finish the case, and the jury will begin deliberations. Again, they deliberate until 4:30, and we'll have further discussions about what the Court expects the parties to do.

Now, it might be helpful -- as a matter of fact, it would be helpful, is, tonight, before you leave, because you've got a little bit more than half an hour before we recess, to inspect the jury exhibits. Because I'm going to ask you again tomorrow to inspect the exhibits to ensure that only the admitted exhibits will go back to the jury room. The burden is upon the parties to go through your list. If it's different from the Court's, you can certainly let the in-court deputy know that. She'll certainly bring it to my attention.

Other than that, I have no other comments.

Counsel for the government, anything else?

MR. BARBOSA: No, Your Honor. Thank you.

THE COURT: Counsel for the defense, anything else?

MR. BROWNE: No, Your Honor.

THE COURT: We'll be in recess. Have a good evening.

(Adjourned)

(End of requested transcript)

* * *

I certify that the foregoing is a correct transcript from the record of proceedings in the above matter.

Date: 8/23/16 /s/ Andrea Ramirez

Signature of Court Reporter